Acceptance of a semi-public digital life worries privacy advocates

March 31 2015, by Dave Helling, The Kansas City Star

The government can know about your phone calls, your emails, the way you use the Web.

Private business tracks your clicks. Your boss knows your digital trail. Your online activity is more public than private.

Almost all Americans now realize this. Most still aren't bothered by it.

A poll released this month - two years after startling revelations about the government's digital surveillance capabilities - shows 9 out of 10 Americans recognize their digital lives aren't secret. Yet clear majorities said they weren't overly concerned about the government snooping around their calls and emails.

"I am not doing anything wrong, so they can monitor me all they want," one user told researchers from the Pew Research Center.

That view worries a growing coalition of privacy experts and advocates trying to speed up efforts to block surreptitious peeking into our digital habits.

Their task isn't easy.

Americans - more than Web users abroad, experts say - have come to accept a semi-public digital life. Private businesses make billions of dollars from sweeping up the crumbs of information digital users leave

behind. In exchange for all that secret data, private businesses offer a relatively seamless and low-cost Web experience most consumers prefer.

Privacy software can be expensive and is almost always clumsy. And the government wants in: Citing security concerns, the authorities seek "backdoor" access to email accounts and phone records.

So privacy experts are stepping up efforts to convince consumers of the need for digital privacy. A fundamentally private Web won't be a reality, they say, until ordinary Americans demand broad protection from government and business intrusion into their phone and computer use.

"If anyone in society is going to have privacy, then everybody has to have privacy," said Alan Fairless, CEO of SpiderOak, a company that offers encrypted data storage for consumers.

Some early-adopting digital-savvy consumers have started to seek out and invent privacy protection tools, he said. That work may eventually trickle down more broadly to less tech-handy cellphone users and Web surfers.

It hasn't yet partly because most Americans seem satisfied with their current digital experience. Prices are low and access is simple precisely because users can trade their data for an easy Web experience.

"People are very willing to sacrifice privacy for convenience," said Aaron Deacon, managing director of KC Digital Drive, a local group exploring issues related to Internet use and access.

Pew's research shows that over the past two years - since the disclosures of former National Security Agency contractor Edward Snowden - roughly a fifth of Americans have changed the way they use various digital tools. They change email passwords more regularly, for example,

and turn to programs to obscure Web surfing habits.

Other users manage passwords through websites such as LastPass or Blur, a step security experts say is essential for protecting unauthorized access to your digital trail.

Some users establish different accounts with different privacy goals. Former secretary of state Hillary Clinton now faces criticism for sending and receiving emails stored on her own in-house server in order to protect some communications from public disclosure.

Yet more complicated privacy protection efforts like encoding and decoding emails remain a difficult task for most users. Many abandon the effort, effectively surrendering privacy for simplicity and speed.

The Pew survey found just 2 percent of email users who know about potential government surveillance actually encrypt their digital messages.

"The failure is in making easy-to-use tech," said Mark Jaycox of the Electronic Freedom Foundation, a California-based digital advocacy group. "It's well-known we need to do better at making encryption easier."

A company called ChatSecure, for example, offers free software allowing cellphone users to send coded messages. Yet its developers admit that encrypting even the simplest texts can confuse most of us.

"One of the biggest challenges when creating security software," the company says, "is ensuring it's usable by normal humans."

Even so, the push to simplify privacy protection mechanisms is picking up speed. Major Internet companies such as Google and Yahoo are working on simpler email encryption programs. Other, smaller firms

offer off-the-shelf software that promise user privacy.

"Cybersecurity and privacy applications are a huge emerging market," Deacon said.

Broad use of privacy mechanisms in the digital world could provoke a backlash - from private businesses that make millions from their access to digital data and from the government, which wants quick access to phone calls and emails for security reasons.

"Social media and the Internet is the primary way in which these terrorism organizations are communicating," President Barack Obama said in January. "And when we have the ability to track that in a way that is legal, conforms with due process, rule of law and presents oversight, then that's the capability that we have to preserve."

Some officials have argued for "backdoor" access to encrypted communications, giving the government quiet access to emails and phone calls that users may inaccurately believe are secure.

The idea angers civil libertarians and tech groups.

"We have a good policy standard: the U.S. Constitution," said Jeffrey Mittman, director of the Missouri chapter of the American Civil Liberties Union. "There are limits on the government's ability to search and invade Americans' privacy."

Fairless, with SpiderOak, said back doors for encrypted data are a bad idea.

"Back doors are almost never tightly controlled," he said. "If there's a back door, it's basically impossible to guarantee only the good people use them for good reasons."

A company called Wickr offers free "military-grade encryption of text, picture, audio and video," its website says. It, too, resists efforts for backdoor government access.

"While all governments must protect their citizens, we as citizens and as companies must stand up for one of the pillars of freedom - privacy," the company says.

Concerns about truly private digital technologies aren't limited to governments. Private companies now make millions of dollars by tracking online habits and selling that information to others.

The White House recently proposed a Consumer Privacy Bill of Rights designed to protect online habits from improper use by private firms. The measure would require businesses to tell consumers what data is being gathered - and offer "reasonable means to control the processing of personal data."

Some industry groups have criticized the plan.

"The proposal could hurt American innovation and choke off potentially useful services and products," the Consumer Electronics Association said.

At the same time, Internet advocacy groups say the bill doesn't go far enough.

"The bill should provide individuals with more meaningful and enforceable control over the collection, use and sharing of their personal information," a coalition of digital and consumer lobbying groups wrote the White House in early March.

The tension reflects a central truth about our digital lives: We want

phone and Internet service that's easy, cheap, fast, reliable, safe and private.

Doing all of those things at once isn't easy.

"The way that people want to use the Internet demands that they give up a lot of privacy," Deacon said.

"People want two different things that are sort of contradictory."