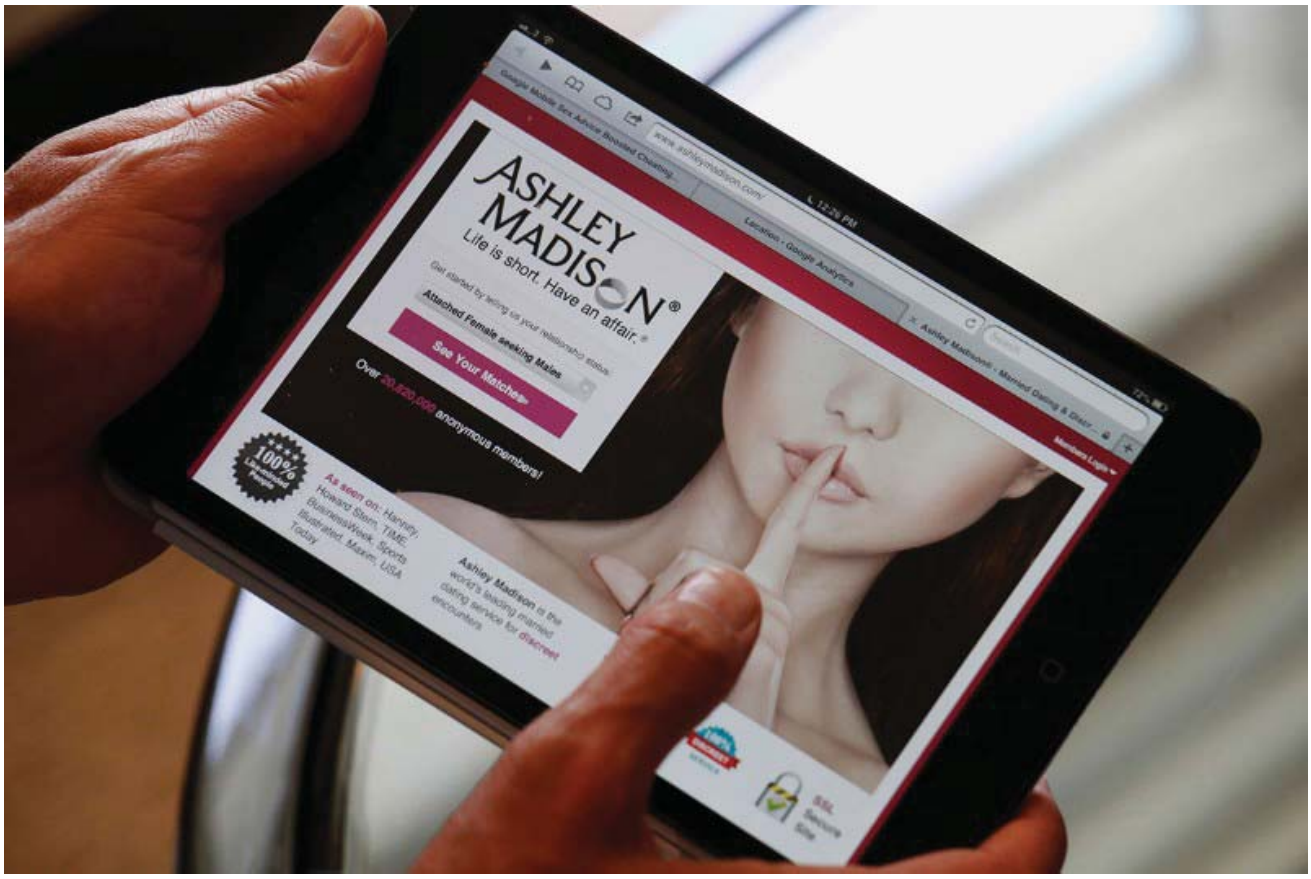
42

SPECIAL REPORT 26 August 2015

# After Ashley Madison: How to regain control of your online data

Recent hacks have exposed just how vulnerable everyone's personal data is. New technologies could change the very basis of how companies store our information




Not so secret anymore *(Image: Bobby Yip/Reuters/Corbis)*

ONLINE privacy as you know it died last week. But the reaction to the release of Ashley Madison's dossier of more than 30 million people seeking affairs was one of muted resignation. "Assume everything you do and say will be made public," one commentator declared. Another bemoaned "the impossibility of perfect privacy". The received wisdom is clear: our data will never be safe.

This collective shrug is the result of security fatigue, says privacy researcher Helen Nissenbaum of New York

University. The companies who store our data have all the power, but the responsibility for protecting it has been placed on individuals. And we're ill-equipped for the job. If you were using the Ashley Madison site, the strongest password in the world wouldn't have kept your details off the growing number of searchable databases now being scoured by suspicious partners and those looking for dirt.

And it's not just members of illicit websites who need to worry. "All of us are shedding data with no clue as to how it is being used, abused, protected – or not," says Nissenbaum. We are simply meant to have faith that the trade-off of our data for what the company offers us is worthwhile, she says.

It is certainly worthwhile for the companies. Sliced and diced and sold to third parties, data can be a bounteous cash cow. What you get out of the deal is less clear. One thing we do know is that the model of trusting someone else to hold your data has failed.

Some researchers think you should revoke some of that trust. "I can't believe people put their real names, email addresses and credit card details on to a website like that," says Krzysztof Szczypiorski, a security researcher at the Warsaw University of Technology in Poland. He thinks the Ashley Madison hack will be a watershed moment for people's understanding of just how exposed their data is. He says people will start to avail themselves of smarter ways of disguising illicit behaviour. Email accounts under a different name, and prepaid credit cards that can be loaded anonymously, for example, "would have saved a lot of people's marriages", he says.

## Question of risk

Instead of people storing and sending unencrypted nude photos, Szczypiorski thinks steganography will become more popular – embedding a nude photo inside an anodyne picture of ducks at a park, say.

But while those options will work for the tech-savvy, Lee Rainie at the Pew Research Center in Washington DC thinks they won't necessarily trickle down to all people. "Even though they are reminded frequently that their data is at risk," he says, "it's pretty clear that many are making only modest changes – if at all."

Sandy Pentland of the Massachusetts Institute of Technology says that putting the onus on individuals is misguided. "It's the data collectors that are the problem," he says. "They have never had any stake in making your data secure."

For Nissenbaum, it's a question of risk. "If a data collector does not provide adequate security, there's a small risk to them and a potentially large benefit."

The spate of recent hacks may be changing that (see "A history of hacks"). Breaches such as that affecting Sony's files last year demonstrate that hacks can damage not only the lives of people whose details are stolen, but also the companies deemed liable for the theft.

Sony suffered financially but survived. Ashley Madison may not fare so well. "Under data protection laws, that case will be a slam dunk," says Patrick Rennie, who specialises in data protection at London-based law firm Wiggin. In the past, it has been difficult to prove damages or distress, he says. "That's not going to be a problem here." Class action lawsuits have been filed in the US and Canada.

"A couple more hacks like this and it will start to change the attitude of the data collectors to holding your data – from cash cow to liability," says Pentland.

Over the past year, there has been growing awareness that "breaches are inevitable", according to IT market research company 451 Research. So what will happen when companies lose their appetite for storing data?

Several protocols are in the works that would change the way personal data is stored. Instead of simply throwing up our hands in frustration every time our data is violated, we could revoke access to it even when it already exists on the open web. It would be the online equivalent of squeezing toothpaste back into the

tube.

“In the current model, the data lives someplace and you have to protect it,” says Pentland. “If you share it with someone, they can run away with it. You can chase them, but it’s pretty hopeless.” So he and his colleagues Guy Zyskind and Oz Nathan have developed a protocol called Enigma, based on the blockchain – the secure digital ledger that tracks bitcoins across the internet.

Instead of having all the data in one place, Enigma constructs a “holographic” version that it breaks into many encrypted pieces and stores in far-flung spots. Anyone can use the Enigma protocol, Pentland says, including Netflix, banks and health providers, but you would be the gatekeeper of your data. You would have the power to give permission to third parties to run queries on it, and the power to revoke that at will.

Think of it as a jigsaw puzzle whose pieces are in hundreds of different places. “No one piece means anything,” says Pentland. “If a thief got their hands on most of it, it wouldn’t make any sense.”

Once you grant access to someone querying your data – say Netflix wanting to check that you are 18 – then and only then do the relevant jigsaw puzzle pieces coagulate to provide the answer before vanishing again.

The system is based on the anti-fraud record securing bitcoins. Anyone who owns bitcoins has an exact copy of the blockchain, making forgeries impossible and removing the need for third parties like PayPal to verify online transactions. Pentland and his colleagues have turned that same public ledger into an access control manager that tracks and verifies your personal data and any queries, permissions and shares.

There are other ideas about how to keep data safe from prying eyes, or from people who don’t want to assume the risk of protecting it. Projects are under way at IBM and Microsoft, whose proposals resemble e-wallets that hold your data for queries but never for direct access or storage.

A version of Enigma will be available later this year, and if such services take off, you truly will be responsible for your own data. At that point, the warnings to guard it will make more sense. “You can still do stupid things under Enigma,” says Pentland. “You could give permissions to the wrong person.” However, without access to the original “hard copy” of your data, he says, it will become impossible for advertisers to use that data without you knowing, or for people to buy it.

Currently, companies that misuse your data can be sued, says Rennie, but you’ll never be able to eradicate data breaches. “You can make theft illegal, but that’s not going to stop someone pinching a bicycle.” Tools like Enigma could be the next best thing.

**Leader:** “It’s not too late to reclaim our privacy”