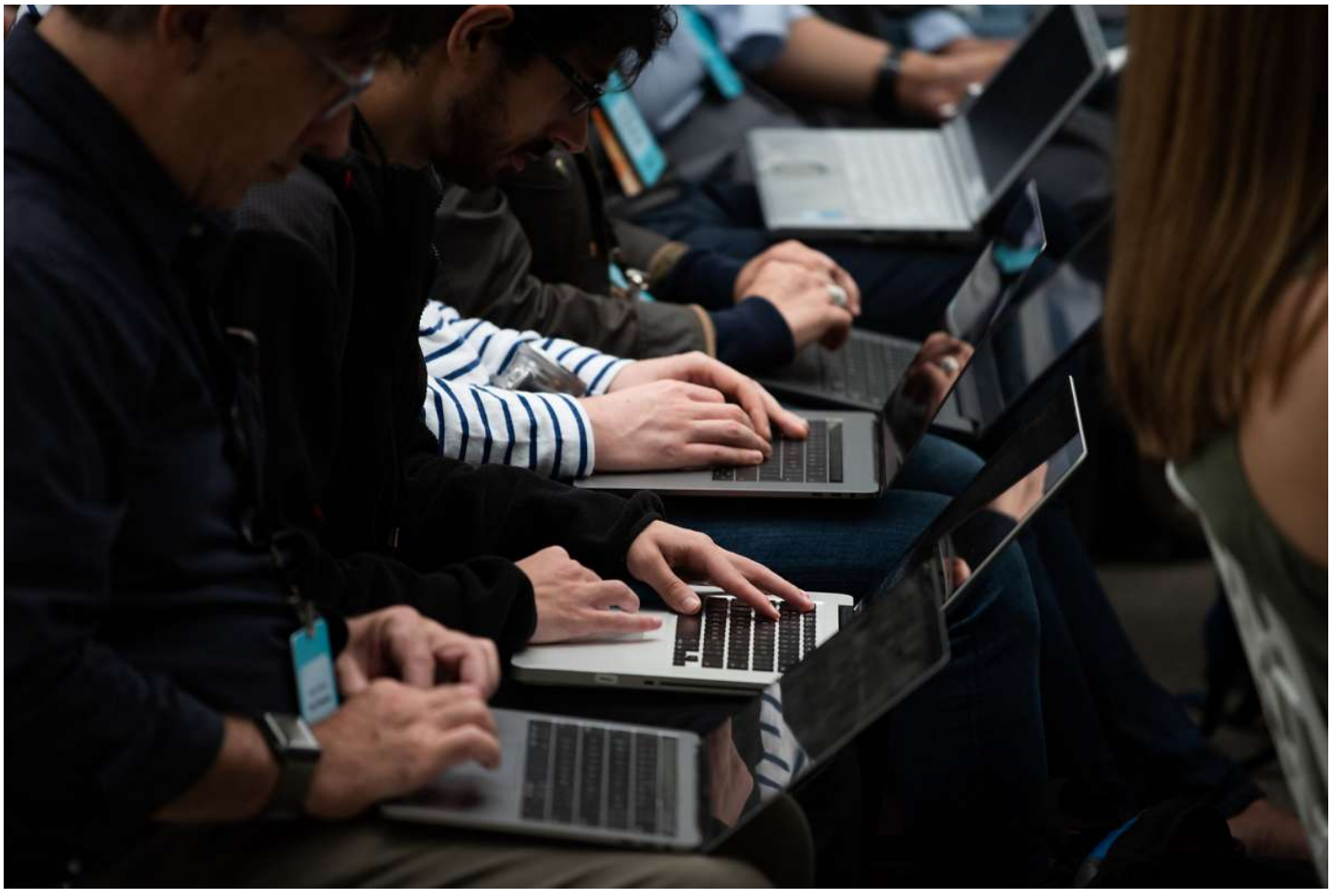
OPINION // OPEN FORUM

Our smart devices must be made to forget us

By Dov Greenbaum and Mark Gerstein

Oct. 18, 2018 | Updated: Oct. 18, 2018 5:52 p.m.



Tech writers take type on laptops during Amazon's release event for new Alexa products and services at The Spheres in Seattle on September 20, 2018. - Amazon weaves its Alexa digital assistant into more services and devices as it unveiles new products powered by artificial intelligence including a smart microwave and dash-mounted car gadget. ...

Photo: GRANT HINDSLEY, AFP/Getty Images

Riveting testimony before Congress these past few weeks may impact America for years to come: Privacy advocates and tech companies have been presenting their conflicting visions for the future of privacy law in America. A noteworthy example of these types of laws is the

new California cybersecurity law, a first-in-the-nation regulation for the information privacy of interconnected devices in the age of the "internet of things."

Unfortunately, the California law fails to oblige manufacturers to ensure that the very devices that you own and physically possess can be easily and completely wiped of all data. It is imperative that any federal law include this emergent necessity.

Why is this so important to you? Selling, donating or trashing unwanted digital devices used to be carefree. You could even lose your device without worrying too much beyond simply the replacement costs and confirming that your backups were up to date. Now things have changed.

With the rise of the internet of things, we now all inadvertently leave some residual private and identifying information on a growing number of our belongings. Even when we attempt to wipe these devices clean of all our data, we likely leave a little data *schmutz* behind.

Considering selling your smartphone? Hopefully the manufacturer will provide you with coherent instructions to erase your device. Without a complete and total wipe, someone could access more than just your recipes and homework assignments. They could determine your passwords, find important and identifying personal information, and potentially health-related or financial data. Just from the metadata associated with your photographs, someone could easily infer where you live, work and vacation.

Unlimited Digital Access for 99¢
Read more articles like this by subscribing to the San Francisco Chronicle
SUBSCRIBE

And those are the most obvious examples.

Selling your car could similarly result in divulging personal information, including past location history, contacts, garage door codes and other data saved on the cars' myriad on-board systems. Some cars offer a factory reset to wipe your data; in other cars, you may not even know how many systems are actually recording your data, or how to erase them.

Here, like for many other internet of things devices, we are essentially at the mercy of the manufacturers. Unlike a computer, you cannot easily find and take out your car's hard drive and erase or destroy it. This involuntary data sharing between consecutive owners is actually a two-way street: in some instances, cars that were sold and supposedly delinked from the

owners' accounts can remain dangerously accessible to the original owners. Likewise, syncing a phone to a rental car or other temporary devices can leave data detritus that is accessible to strangers.

In some instances, manufacturers can even track the secondary lives of a product via a chain of custody linking successive owners to the device's unique serial numbers. That is, as one seller deletes their local account on an iPhone, another buyer appends theirs, effectively creating a connection between two people in Apple's servers. In some instances, that connection is random. In others, it's a relationship that should have the right to remain private.

Even more disconcerting, our data residue may be on other people's devices as well: The leased photocopier at the bank or medical office probably has an internal hard drive that, unbeknown to most, dutifully retains thousands of scanned documents, including health records, bank statements or employment records. Those hard drives may not necessarily be erased when the copier is leased elsewhere, sold or junked.

As devices become ever "smarter," we will leave additional private information on them as well. For example, the latest Apple watch is designed to be an "intelligent guardian of your health" that includes a built-in electrocardiogram. Moreover, Apple is far from the only consumer device company that aims to collect health-related data. This summer, Fitbit released research culled from 150 billion hours of ostensibly anonymous consumer heart data.

Wiping this increasingly private data from all of our devices before resale or disposal has become an imperative, albeit increasingly onerous, undertaking.

While business opportunities will abound for companies to purge data from old products, more fundamentally, consumers should be entitled to know what data is stored on each device and how it can be wiped. Similar in spirit to the new European privacy regulations, which mandate privacy by design, all devices should be designed to make this data cleaning stress-free.

Beyond the amorphous digital *schmutz* lurks an even more insidious data leak. In the near future, substantial data will be extractable from genetic material left on sold or discarded items — a sweater, some kitchen items, or even your now digitally clean internet of things device. Like the data on your phone, this genetic data can be used to characterize a person or even their ancestry, and link them with other genetic information publicly available in large repositories.

While the concerns regarding genetic data remain a couple of years away, digital data *schmutz*, however, is an immediate concern. And while market forces will hopefully push manufacturers to help consumers clean their devices, optimally, the next iteration of Europe's "right to be forgotten" will include the right for the devices you own to forget you.

Dov Greenbaum is director of the Zvi Meitar Institute for Legal Implications of Emerging Technologies. Mark Gerstein directs the bioinformatics lab at Yale University.

HEARST *newspapers*

©2018 Hearst