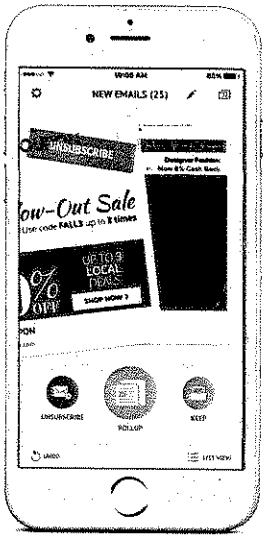
Privacy: The downside of 'free' apps

It's "a Silicon Valley tale as old as time," said **Brian Feldman** in *NYMag.com*. A technology company comes along offering a handy service that just so happens to be free. Users sign up in droves. Then it's revealed that the company has been harvesting and selling their data, and those same users revolt. This time, the pitchforks are out for Unroll.me, an app that scans users' email accounts to unsubscribe them from junk mail. *The New York Times* recently reported that Unroll.me scanned its users' email for Lyft receipts and sold the anonymized data to Uber to help that firm keep tabs on its ride-hailing rival. The revelation was a minor detail in a bigger profile on Uber CEO Travis Kalanick, but it sparked the predictable firestorm on social media, with users angrily denouncing Unroll.me. The company's response was just as typical: Don't blame us. "It was in the terms of service."



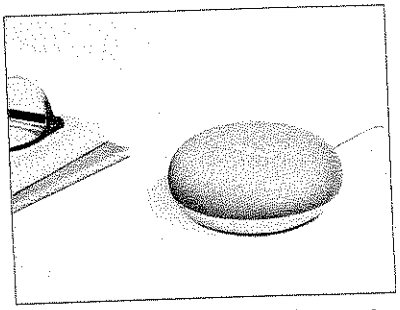
Unroll.me comes with a 'price.'

What exactly is the big deal? said **Stephen Bronner** in ***Entrepreneur.com***. Internet users "should be savvy enough by now to know that there is no such thing as free." Unroll.me warned users in its privacy policy that it might sell their data, but there's also nothing wrong with asking for something in return for providing a useful service. Unroll.me employees "need their paychecks, and I need a less cluttered inbox." Still, Unroll.me didn't do itself any favors with its tone-deaf response, said **Ashley Carman** in ***TheVerge.com***. One co-founder even wrote an angry blog post asserting that if Unroll.me's critics were shocked by the company's data collection, "they have clearly been living under a rock." The post was "insensitive," but it "has a point." Nearly every major tech company makes money from user data. Why do you think your Gmail account is free?

But just "how open was Unroll.me about what it does?" asked **Kashmir Hill** in ***Gizmodo.com***. As with most tech companies, its privacy policy is buried in pages of impenetrable legalese nobody can realistically bother to read. By one estimate, internet users would have to take an entire month off work to read through the terms of service agreements for all the apps and websites they use. Unroll.me's agreement is particularly egregious, warning users in fine gray print of its vague plans to gather "non-personal information" to "build anonymous market research products and services." Whatever that is, it's not a clear explanation of Unroll.me's business model. Take this uproar as a reminder to check the permissions you've given various apps to access your email and social media accounts, said **Brian Barrett** in ***Wired.com***. Once again, the tech industry adage holds true: "If it's free, you're the product."

Smart-home devices: Google's latest privacy mess

"The paranoid nightmare of a voice assistant spying on you is no longer a theoretical," said **Eric Limer** in ***PopularMechanics.com***. Earlier this month, tech blogger Artem Russakovskii was given a premarket Google Home Mini smart speaker to review. The device, which went on sale this week for $49, is Google's answer to the popular Amazon Echo, using voice-activated artificial intelligence to let users check the weather, play music, adjust smart thermostats and lightbulbs, and more. After a couple of days, Russakovskii noticed the Mini "behaving weirdly"; even when he hadn't activated the device by saying "OK Google" or tapping the button on top, the gadget appeared to be turning on all the time, and even reacting to TV programs. That's when Russakovskii checked his Home Mini's logs: The device had been "eavesdropping on him 24/7 and sending all its recordings home to Google." The company blamed a faulty top button for the self-activation, said **Dave Smith** in ***BusinessInsider.com***. But the problem clearly wasn't limited to Russakovskii's gadget, because the company has since disabled the top buttons on *all* Home Minis. This spying "fiasco," coming just as the devices hit the market, is clearly "a black eye for Google's smart-home efforts."


Google Home Mini: Always listening?

The fast-growing market for digital home assistants "needed something like the Google Home Mini disaster to happen," said **Leonid Bershidsky** in ***Bloomberg.com***. Naysayers who have warned of the dangers of putting such devices in our homes are routinely dismissed as paranoid; Russakovskii, before his own incident, admitted to calling such doubters "tinfoil-hat wearers." But these gadgets are designed to listen all the time, and they don't have to be defective for spying to occur. Recording can be triggered "by a hack, an accidental noise, a software glitch." And this is not a problem that threatens a small number of tech enthusiasts. This year, 36 million Americans will use a voice-activated assistant device. "What happened to Russakovskii merely confirms Murphy's Law: Anything that can go wrong will go wrong."

Even without spying, Google's smart-home speaker will have access to a "gold mine" of personal data on you, said **April Glaser** in ***Slate.com***. It will know "when you wake up, what items you need around the house, the music you like, how many other people live at your house, your eating habits, and more." Is the convenience of hearing whether it's going to rain or being able to turn off a lamp with your voice really worth giving up all that information to a company that made $79 billion last year on digital ads? "I'd be shocked if the company doesn't find some way to leverage the data it collects about customers in the privacy of the home to help advertisers better target people." The more I think about it, "I'm cool just dimming the lights myself."

Departments realizing benefits of body cams

Bambi Majumdar Wednesday, September 06, 2017

Photo Caption: Body cameras will soon become a necessary part of an officer's gear. (Image: Axon)

Sometimes the headlines say it all. The Fontana Police Department in California recently announced body cameras as an essential part of their gear. Local media reported it as FPD "joining 21st century policing" with advanced tools.

That's what body cams have become today — advanced tools to help in better policing. The technology is being rapidly adopted by agencies across the nation and will soon become a necessary part of an officer's gear. Many law enforcement agencies hail them as tools to enhance public safety and understanding.

Initially meant to appease upset communities over questionable policing practices, body cameras soon became a useful tool for officer safety as well. These advanced body-worn cameras are designed to document incidents in different and unbiased perspectives, which benefits officers and citizens alike.
Officers who use these regularly have admitted that there has been a drop in not just the use of force but also in the number of complaints against officers. It is no wonder that body cameras are fast becoming mandatory for departments across the country.

Axon's latest camera system in Charlotte, North Carolina, makes usage simpler. The body camera and in-car camera automatically turn on when the blue lights turn on. There is no waiting, no hesitation, no deliberation — taking the burden off the officers. The cameras are also designed to automatically turn on if an officer draws a Taser or firearm.

Responding officers will have their cameras turn on automatically with no action from the officer. In tense emergency situations, this feature can be a boon for officers who can now focus on the situation and not worry about breaking protocol. The collective footage from all officers at the scene can offer multiple perspectives of the same incident for the authorities and investigators.

But companies are still innovating. In the near future, we may see the human heartbeat come up in the footage as well. Since respiration and pulse go up under stress, the camera in future would record these vitals to signal the headquarters when officers are in trouble and need help.

Cash-strapped departments like Jersey City, New Jersey, are not letting the budget get in the way. They are the first to test the viability of using cellphone cameras as an affordable alternative to body cams. Officers on patrol, pursuing a suspect or in any community interaction will strap on gear that will include a body camera in a cellphone.
The police-issued cellphone will be set to a mode to function as a cop camera. When turned on, the recorded footage will directly stream onto a secure server at the police department. The app that will use the less-expensive method, CopCast, comes from Google's sister company Jigsaw.

The latest body camera technology is meant to strengthen officer accountability and public trust. Some departments have been quick to adopt this technology, while others are slowly getting budget nods.

Sooner than later, officers from coast to coast will need to wear them when on duty.

From MultiBriefs, which provided content for a September 13th, 2017 International Union of Police Association newsletter:
http://exclusive.multibriefs.com/content/departments-realizing-benefits-of-body-cams/law-enforcement-defense-security.

CHINA

The iPhone is a gift to autocrats

Eugene Chow
The Diplomat (Japan)
Sept 8. The Week

The Chinese government has long sought the means to keep closer tabs on its citizens, said Eugene Chow, and it now has the perfect tool through which to do it: the smartphone. These ubiquitous devices provide an instant window into people's browsing history, purchases, and location. Nearly 80 percent of all smartphone owners in China, for example, use an app called WeChat. Far more than just a messaging app, it's a hub through which people access the internet and other services; they use it to pay bills, check flights, get bank statements, and make doctor's appointments. While U.S. law restricts the government's ability to spy on citizens' browsing habits, Chinese law doesn't—and the Chinese government has made no secret of its efforts to integrate such data into its surveillance apparatus. Indeed, it's planning to create a "social credit" rating system that will draw on exactly such databases, logging what individuals buy and look at on the web, and noting infractions such as failing to keep up with bills or violating family-planning rules. Those with low scores will have a harder time traveling and will be barred from certain privileges. The "technologies that once promised freedom and openness" are helping China's authoritarian rulers build a "digital panopticon."