Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security

CR partners with other cyber experts, creating a new open-source industry standard to make connected devices safer

By Consumer Reports

March 06, 2017

One day in August 2015, Jared Denman got a frightened phone call at work from his wife, who was home with their 2-year-old daughter. A song was playing through the couple's baby monitor—the Police's "Every Breath You Take." The monitor was the kind that connects to the internet so that parents can see and talk to their baby or caregiver when they're away from home. The device had been taken over by a malicious hacker, and the song's lyrics were particularly ominous: "Every game you play, every night you stay, I'll be watching you."

Incidents like this may illustrate the need for consumers to be better educated and more vigilant when it comes to digital security. But if a breach could happen to Denman, who is an IT administrator with a sophisticated understanding of computer security practices, it can probably happen to most consumers. Some products, like the Denmans' baby monitor, are sold by their manufacturers with vulnerabilities that leave them open to attack, such as a setup process that doesn't require users to change the default username and password. And it's not just homes with baby monitors that are vulnerable. It's also homes with routers, security cameras, health-and-fitness apps, and even cars.

These types of attacks “are probably happening to more and more people, and they don’t know anything about it,” Denman says.

In our recent CR Consumer Voices survey, 65 percent of Americans told us they are either slightly or not at all confident that their personal data is private and not distributed without their knowledge. We think it’s unfair and unrealistic to expect consumers to constantly play defense when the products and services they use aren’t engineered with basic privacy and security protections built in. Consumer Reports regularly writes about major security vulnerabilities and offers advice to our readers about good practices that can help protect their data and privacy. But as an organization, we aim to do more.

That’s why we’re now launching the first phase of a collaborative effort to create a new standard that safeguards consumers’ security and privacy—and we hope industry will use that standard when building and designing digital products such as connected devices, software, and mobile apps. The goal is to help consumers understand which digital products do the most to protect their privacy and security, and give them the most control over their personal data. This standard can also eventually be used by CR and others in developing test protocols to evaluate and rate products—which will help consumers make more informed purchasing decisions.

We know we’re not the first ones to try to move digital products and services in the direction of greater privacy and security. In the past couple of years, efforts have been launched by both government agencies and other private organizations to pull together guidelines, but these have usually been narrowly focused on a single area, such as privacy policies or the security of connected devices. None of them has gained wide support. And some protections are actively being rolled back—the Federal Communications Commission (FCC) recently blocked a new rule that would have added data security protections for internet users.

Consumer Reports has been working with several partners and has taken a comprehensive approach, building on some of the best thinking that has gone into prior efforts. We think these standards address a real gap in the marketplace. Here’s an overview of how this project came together and how these standards will work.

Illustration: Oliver Munday

What's the Point of a 'Standard'?

Look around, and you'll see product standards in just about every field. Their purpose is to define what good products have in common, and these standards generally evolve over time. For instance, current federal safety standards ensure that vehicles have seat belts, multiple airbags, and electronic stability control to help protect drivers and passengers.

Standards and test protocols to evaluate products can be created by government agencies, but they don't always have to be, especially if the government is not adequately addressing a problem in the marketplace. Consumer Reports has plenty of experience working with and advocating for stronger standards for all manner of products. We pushed hard for and provided scientific input on the development of dynamic rollover tests now used by the government to evaluate all cars, including SUVs. We also develop our own protocols when we believe existing standards are not going far enough to protect consumers. The safety protocol we developed for doing comparative crash-testing on child car seats was designed to reflect consumers' real-world experiences better than government tests, and it has spurred a lot of productive dialogue with manufacturers.

We are now turning this type of focus to privacy. If Consumer Reports and other public-interest organizations create a reasonable standard and let people know

which products do the best job of meeting it, consumer pressure and choices can change the marketplace. We've seen this repeatedly over our 80-year history.

Maria Rerecich, who directs electronics testing at Consumer Reports, is helping lead the project. "All kinds of products and services collect consumer data and rely on software to work," she says. "But no one has defined how companies should build these products to really be good for consumers in terms of privacy and other issues." Those products include such diverse items as smart TVs, routers, security cameras, thermostats, and digital assistants (think Amazon Echo and Google Home)—as well as pure software products such as apps and web browsers.

Getting this right matters more than ever. Even though internet-connected washing machines and automobiles may seem like high-end novelties today, these devices—as well as the apps and services that support them—are quickly becoming the norm. Two years ago, about 40 percent of the TVs for sale were "smart" or "connected" sets, according to Gap Intelligence, a market research firm. By December 2016, the number was about 60 percent, and it's sure to rise further. Appliances such as slow cookers and refrigerators are starting to incorporate that kind of connectivity as well.

Our Privacy Standard—A Quick Overview

What does our digital consumer-protection standard ask of companies? As an example, we think devices that connect to the internet, such as the Denmans' baby monitor, should require consumers to choose unique usernames and passwords during setup. You can't create an online bank account without creating a secure password; that should be true for a camera that transmits video from inside your home as well.

The new standard also calls on companies to delete consumer data from their servers upon request, to protect personal data with encryption as the data is sent through the internet, and to be completely transparent about how personal consumer information is shared with other companies.

This standard ultimately can be used to help Consumer Reports and other groups

develop specific and repeatable testing procedures. Then we can evaluate products and give consumers the ability to compare products against each other on the basis of factors such as privacy protection, the way we already give them information on other aspects of product performance. In the hands of consumers, that kind of information is a powerful tool. It can help the individual, and it can shape the future.

> Check Out CR's Guide to Privacy

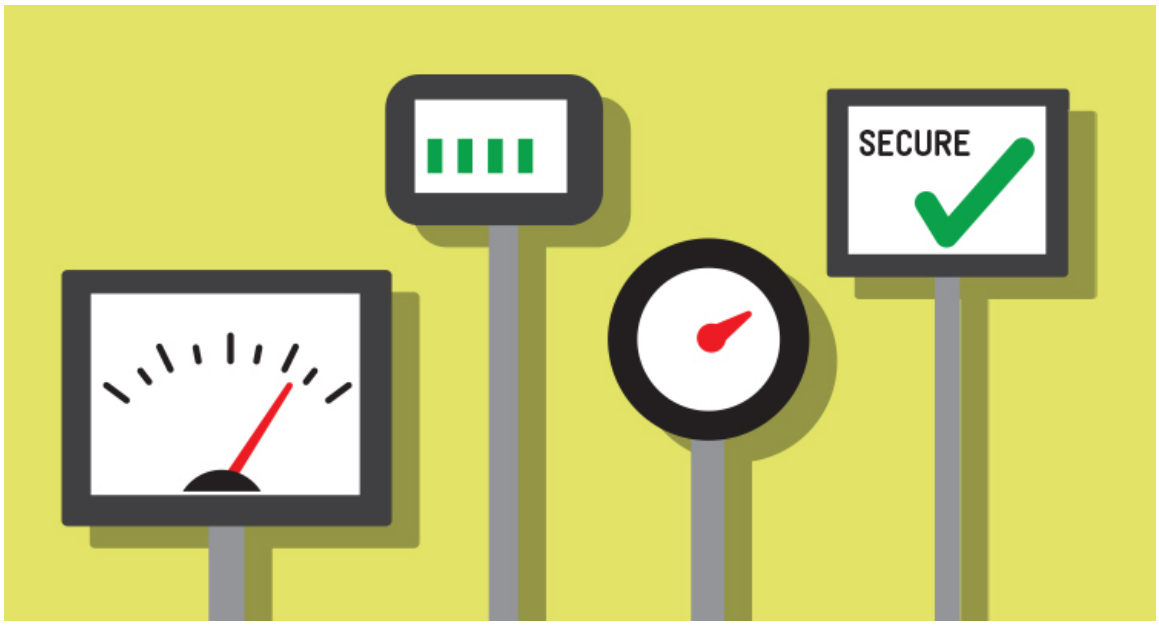

Illustration: Oliver Munday

Built Through Partnerships

We collaborated with three of the digital world's most highly regarded leaders in the area of consumer protection: Disconnect, a company that makes digital tools consumers can use to block data-trackers and prevent other invasions of privacy; Ranking Digital Rights (RDR), a nonprofit research project that pores through privacy policies and other information that companies disclose to users; and Cyber Independent Testing Lab (CITL), a nonprofit software security-testing organization.

CITL was founded by info-security expert Peiter "Mudge" Zatko and mathematician Sarah Zatko. "The security community has been trying for years to get people to care more about software security, and now people finally do," Mudge says. "But the security community is not providing consumers with

meaningful things to do about it. You cannot tell people everything's on fire, and then not have anything positive for consumers to do. We want to give all types of consumers the information they need to make smart security and safety decisions on what products to choose and use."

That can empower consumers—and give companies a new way to compete with each other. "We've found that companies have very different approaches to protecting privacy and freedom of expression," says Rebecca MacKinnon, the founder of Ranking Digital Rights. Establishing an industry standard, she says, is the best way to "encourage companies to act more responsibly."

To create the standard, all of the partners in this effort met repeatedly over a period of months to forge a working draft. Then each organization took different portions for trial runs by applying them to real products. The group looked at smart TVs, web browsers, and ride-sharing apps. Some of Disconnect's tasks were to observe network traffic generated by the products to identify the presence of data trackers, determine whether private information had been encrypted, analyze permissions, and look for any egregious privacy violations.

RDR focused on privacy policies across all three product categories, CITL evaluated the browsers to see how securely they were built, and Consumer Reports analyzed multiple product categories to see whether they were susceptible to known security vulnerabilities. The idea was to refine the standard by using it for real-world evaluations.

"Together with our partners, we're embarking on this ambitious journey to ensure that consumers remain in the driver's seat when it comes to the safety and security of their personal data," says Marta L. Tellado, President and CEO of Consumer Reports.

This is just the start of the conversation. Consumer Reports and our partners don't own the standard—no one does. We're releasing it in a public, shared document. And we're inviting others to give us feedback, add their own ideas, and make the standard better.

Our Supporters

Building out a product standard and testing program is important and difficult work that requires expertise. It is also expensive work. CR's testing, investigative work and research is largely funded by donations and member subscriptions. But to launch this program, we have benefited from the vision and generosity of The Craig Newmark Foundation and Craig Newmark Philanthropic Fund, as well as the Ford Foundation. Craig Newmark is a board member of Consumer Reports. The bequests of Henry and Edsel Ford established the 80-year-old Ford Foundation, but the philanthropic organization is today entirely independent from the Ford Motor Company.

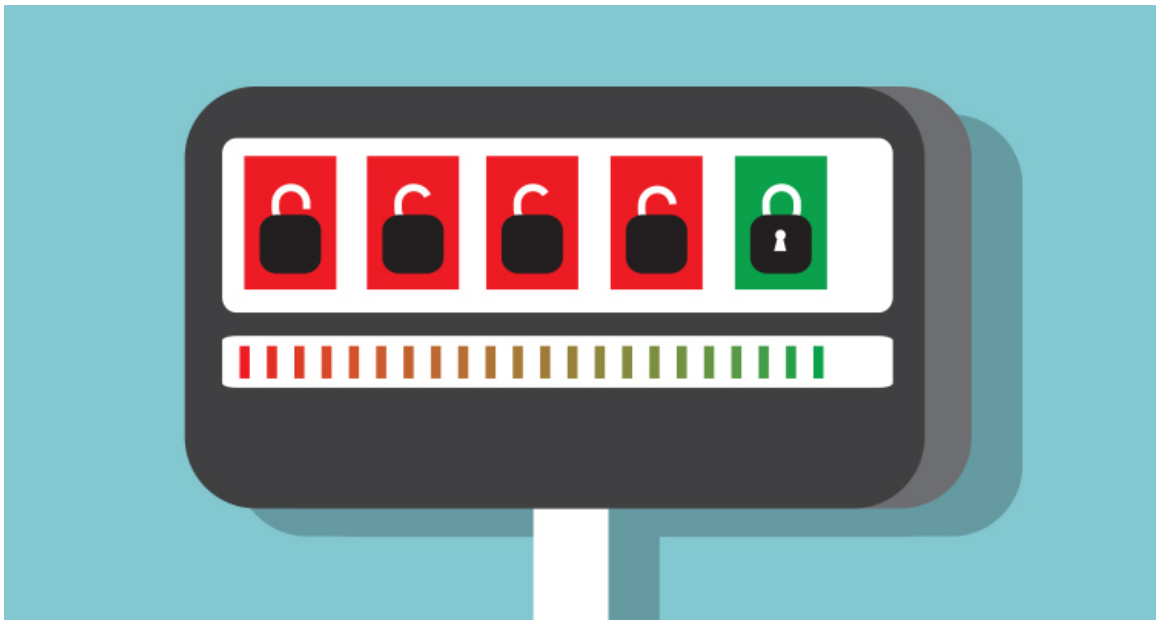

Illustration: Oliver Munday

More Details About the Standard

The full standard fills up several long, complicated spreadsheets. But if you'd like a simplified version, here's an overview:

1. Products should be built to be secure

In the past two years, security researchers showed they could remotely hack into vehicles, taking over the steering and braking. And criminals have repeatedly gained access to laptop webcams, routers, and other products. Bad actors will probably always be with us, so consumers deserve products that are built with security as a priority.

How our standard addresses this. One way to test the security of a system is to ask an expert to break into it and see how hard that is to do. Consumer Reports may engage in that kind of “penetration testing” for some of our projects. But that type of research is time- and labor-intensive, so it’s impractical if you want to evaluate a large number of products.

To quickly check the security of many pieces of software, CITL has built automated tools that detect whether well-accepted security practices have been followed that reduce the risks from attackers, malware, and other threats.

Mudge likes to compare software to automobiles. You can't design a car that's 100 percent safe, he says, but you can follow procedures that are known to improve safety. “If you have a car that doesn't have airbags, seat belts, or antilock brakes, you, as the consumer, need to know this,” he says. CITL's tools check whether a piece of software has the equivalent of such safety features, and evaluates how well they appear to be built and deployed. A good grade from CITL doesn't mean the software can't be hacked at all, but it does mean it was built to be more secure, and tougher to attack.

Consumer Reports will look for ways to incorporate CITL’s tools, as well as other security methods, into our testing.

The standard also asks some pretty straightforward questions, such as whether consumer data is encrypted to protect it from criminals and whether the company behind the product continually updates its software with security patches as new kinds of malware emerge.

2. Products should preserve consumer privacy
In 2015, Consumer Reports found that smart TVs, the kind that connect to the internet, were collecting information on everything their owners watched. We think consumers should know what data of theirs is being collected, and have a reasonable amount of control over it.

How our standard addresses this. The standards ask several questions of any product or service that collects data on its users. For instance, does the company tell the consumer exactly what data is being collected? Is the company collecting that information to make the product or service work correctly, or for some other

purpose? And when a consumer closes an account—quitting a social media service, for instance—does all that data get deleted?

3. Products should protect the idea of ownership

If you own a pencil, you can share it, give it away, or break it in two and write with the stubs. But the concept of ownership has become muddled when it comes to products that use computer chips and software. For instance, many cars, appliances, and even farm machinery rely on copyrighted software to work, and because it's illegal to tamper with copyrighted programming, consumers can be forbidden from diagnosing and repairing machines they've bought—or hiring an independent shop to do the work. Copyright laws are important, but they can also be abused. In general, when consumers buy products, we think they should be able to alter, fix, or resell them.

How our standard addresses this. The standard looks at a number of questions related to ownership. These include whether consumers are allowed to fix an item themselves or have an independent repair person fix it, whether the company tries to prevent the user from reselling it to someone else, and whether the company is clear and transparent about why and when it might unilaterally shut down a user's access to a product or service they purchased or use.

4. Companies should act ethically

The first three statements are intended to create a framework for assessing how companies that produce digital products respect and protect their own customers. The fourth statement holds those companies accountable for how they interact with the broader world.

Why? We think that just as many consumers want to know whether their clothing is made in the USA or whether their coffee was produced using fair-trade practices, they may also care about values such as free speech. For example, a company's customers might want to know whether it resists digital censorship in totalitarian countries, and, closer to home, whether it quickly notifies the public after a data breach.

How our standard addresses this. The details depend on the type of product or service you're looking at. Questions include whether privacy policies are easy to find and to understand, whether a company you do business with is forthcoming

with information if it experiences a data breach, and what kinds of measures it takes to protect freedom of expression.

Photo: Oliver Munday

What's Next

Making our consumer-protection standard public isn't just a gesture of transparency (although we think that's important). It's an essential part of the whole project.

The standard as it's now written is a first draft. We hope that everyone from engineers to industry groups to concerned parents will get involved in shaping future versions of it. We've placed the standards on GitHub, a website that's widely used by software developers to share ideas and work on group projects. Because GitHub can be hard for newcomers to navigate, we've also built a website that has the same information.

Some people might just make suggestions, while others may branch off and experiment with alternative proposals. We encourage feedback and refinement.

What matters for now isn't that every detail is correct. The important thing is for the idea of a digital consumer-protection standard to take hold. Casey Oppenheim, a co-founder and CEO of Disconnect, points out that the new standard could touch on a vast array of engineering practices and privacy

policies, for thousands of products.

“If people think we’ve missed the biggest thing, or gotten something wrong, we’ll be like, ‘Great, let’s talk. We want to improve this with you.’”

What ultimately emerges should be a clear set of best practices that reflect basic consumer rights to privacy and security, and more. The details will evolve as rapidly as the technology and the public debate over these concerns.

The standard should be easy enough for consumers without a technical background to understand, yet sophisticated enough to guide testing organizations such as Consumer Reports as we develop precise testing protocols. We want to rate products on measures such as security, in much the same the way we currently assess products for physical safety and performance.

That will give consumers the power to make choices based on solid information. When consumers vote with their wallets and their clicks, we’ve seen that companies pay attention. We think companies will strive to out-do their competitors when it comes to privacy, security, and other consumer rights. The ones that do a better job will gain more customers. That’s one of the primary ways that consumer power works.
