

Let's put a chip in everything and see what happens

Internet of Unnecessary Things

April Fool's Day has come and gone, but anyone checking out the latest inventions might imagine that it's become an ongoing event. Every day, some familiar device that's worked just fine in the past gets a chip installed to make it "smart". Suddenly, the stupid thing's interactive, not only generating data uploaded to the internet but receiving downloaded commands in return.

Welcome to the **Internet of Things**, this brave new world where *everything* is connected online, giving users the ultimate in instant convenience. A world where a **refrigerator** can show what it holds or display recipes and the **TV responds** like a genie to spoken demands. Too bad they and many other devices can be easily hacked.

This future is already here, only there's one tiny little problem. In their rush to wire everything, many manufacturers have not fully thought out the solutions to basic questions of practical utility while overlooking the most essential safeguards of privacy and security. So along with a lot of new-fangled gizmos which raise puzzled questions of "why bother?", come new problems in how these things can be used or interact which have never been imagined before.

The lure of knowledge and control

"Knowledge is power." The more data to which one has access, the more power one possesses, too. But there can be too much of a good thing.

Few things are better on a hot day than cool, clean water. **Smart bottles** deliver that and so much more. The **Hydra** comes with Bluetooth speakers, a microphone, even a flashlight and mood lighting, while the **Sportline Hydracoach** calculates and monitors consumption for athletes and coaches based on weight, weather, altitude and health conditions like pregnancy.

Then there's the **Thermos** with a "smart lid" to track beverage temperature, quantity, and hydration progress. (Just be careful not to get the USB port wet.) Or the **Pryme Vessyl**, which has a white line on the side to indicate water level, and a reassuring blue light on the lid to show when the user is properly moist.

Many other smart bottles all do the same thing in slightly different ways, often working through smartphone apps. They're *not* cheap either, the **top 10** ranging from \$25-100, averaging at about \$55 each. Plus, most have apps that have to be configured with the users' personal data to be at all useful, and inevitably will have to be recharged or have their batteries changed.

But really, apart from athletes in rigorous training or people with certain delicate conditions, who *needs* this stuff, or the hassle using it? Yet, the same thing is going on across the entire vast swath of personal, household, and health products. How about **smart dental floss**? There are hundreds to choose from on Amazon. **Smart bathroom scales**? – even more listed on Google.

From **smart breast pumps** and **hairbrushes** to **cutting boards** to **clothes dryers** to **shoes that lace themselves**, just about *any* product imaginable can, and will be, hooked up online – even those where security is the primary concern.



There are **smart door locks** which not only are supposed to operate without keys even remotely, and send alerts on entrances and exits, email limited-access keys to guests and workers.

Instead of a key (which should be carried as a backup for some models), a smartphone or special fob is generally needed for access. The **Yale Assure**, for instance, is completely keyless and thus cannot be picked while the **Kevo Touch-to-Open** needs just a tap, and it can network with the home's **Nest smart thermostat**, too.

Remote control of physical access is just the start. The great dream is of **integrated smart homes**, where *all* the various systems can be controlled from afar, where doors, lights, windows and drapes work with heating and cooling to keep the internal environment comfortable.

Of course, it will be **new homes** built with smart systems in mind where this will first happen. **Older dwellings** will require more piecemeal adaptations. But one point where smart systems are already making an impact on all types of homes is at the power source, with smart meters.

Smart meters are being heavily **promoted** by the electric industry and the government. They record power consumption in near real-time, reporting results back to the power company. This is to gauge energy usage, making billing more accurate, allowing consumers to efficiently manage their own patterns and save money. But there has been a lot of not-entirely-irrational consumer suspicion stubbornly **pushing back**.

Privacy and **security** concerns are part of it, plus fears of the **health effects** of the radio link, but what raises the greatest anxiety is that most of these meters carry a remotely controllable **kill switch** allowing the power company to turn off the juice entirely at will. This could be needed to save the grid during a brown-out or other emergency, but what about unpaid utility bills?

Overbilling is indeed the most widespread concern – one **survey** reported that a third of users had their power bills increase after installation. More serious fears, however, are related to the **security of the power grid** itself, especially now that generation systems have been **hacked**.

Yet the desire to connect to the net is irresistible. A recent model **Meile commercial dishwasher** had a web server installed for remote access. The

password folder however was easily hackable. Intruders were able to not only take over the system but use it to disseminate malware.

When things go bad

This situation is not at all uncommon. **Botnets** comprised of millions of unsecured devices have already figured in massive **denial of service attacks** against major internet providers. At one unnamed **university**, a botnet of campus vending machines and over 5000 smart bulbs was used to attack the school's own computers.

Typically, warning signs were ignored. Sadly, such indifference to **security** is the norm for smart things, not the exception. In few if any of the glowing descriptions of online-connected products can any mention of security be found.

This complacency is alarming and **dangerous**. **Shodan**, a search engine for the Internet of Things, lists countless open baby and web cams as well as power plants and refrigerators, while a recent **Wikileaks dump** outlines methods the CIA can use to eavesdrop through **smart TVs**.

Even toys aren't safe. **CloudPet** teddy bears that recorded and forwarded voices so absent dads could talk to their kids had millions of recordings repeatedly leaked and held for ransom.

Well-designed, useful smart things are truly beneficial. But they can be turned to evil when they turn people into things. For instance, health care workers now must be alert for RFID chips implanted in **human trafficking** victims. 

SWCP customer data will not be sold

The FCC now **allows ISPs** to sell their customers' browsing and other data. **SWCP's Data Policy** remains the same as it always has been: We do not sell customer data to anyone for any reason.

Check our **blog** to see who might, though.



Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994

505-243-SWCP (7927) © SWCP.com © Help@swcp.com

5021 Indian School NE, Suite 600, Albuquerque, NM 87110

Archived at: <http://www.swcp.com/newsletters/>.
Click on **blue terms** in PDF file to open links.