Good idea, but maybe needs a little more work.

What could go wrong?

Technology keeps evolving ever faster. The world today is full of amazing things like the internet which were unimaginable a century ago. Change constantly accelerates with new ideas sprouting everywhere. Nowhere is this more visible than on the web.

Among all these shiny new devices and programs being developed all around us are a number that really should have been thought out better. Many of the problems that rapid technological change has brought about are due to too hasty implementation without proper evaluation of possible downsides.

It's one reason why computer programs are buggy, systems require frequent patches, and every day brings new hacking exploits. But in such a whirling churn of possibilities, quite often the best idea seems to be to toss everything into the pot and let the market sort it out. What could possibly go wrong?

Quite a lot. Take gene editing for example. **CRISPR** is a technique to edit genes easily by snipping out or adding DNA like a word processor. The **potential** to cure fatal cancers and eliminate genetic diseases within the body is revolutionary. Scientists around the world are trying it out on many diseases already.

And not just scientists – you can **buy a kit** to play with genetic engineering in **your own kitchen**. Sure, there's been debate as to whether CRISPR produces **unwanted mutations** plus serious **warnings** by the FDA against DIY genetic therapy, but if you might get those gills you've always wanted, what's to stop you?

Dubious ideas and driverless cars

Self-driving vehicles are another great idea, which when perfected will allow people to get where they want to go without ever interrupting their texting. But there's a huge pile-up of problems in the way.

First of all, **humans** react far too slowly to ever take over in a crisis. So the cars themselves will have to be able to predict the behavior of everything around them. Sooner or later some idiot will try playing "chicken" against them, but just the mere presence of self-driving vehicles will make our **bad drivers** here **crazy** since driverless cars will obey all traffic laws.

What happens once you get to your destination? If there's no parking, why not set it to circle the block until you get back? Such practices would quickly trash **promised advantages** like saving gas and reducing congestion. The cars will need to have a built-in ethical sense, too, as they will have to be able to deal with life and death decisions at any instant.

Finally, driverless cars are **dream targets** for hackers and terrorists but since lives depend on them, security *must* be impregnable. The Christmas market attack in Berlin last year that used a truck had so few casualties because the stolen vehicle was equipped with a primitive system to **stop automatically** after a crash. But what would happen if a smart 18-wheeler was hacked to *aim* at pedestrians instead?

Many times innovations are taken for granted. **Cloud computing** – where data is stored not in a specific server but a linked cluster of them – is one of these, offering savings and convenience for users relying on big datasets. Often, however, the data is not encrypted or well-protected and is openly accessible.

What is Jeff Bezos thinking?

Amazon is a huge company, an innovator in online shopping, and has made **Albuquerque-born** Jeff Bezos the **richest man in the world**. The company is also branching out, seeking to dominate many other services, including that of cloud computing.

Yet white-hat hackers exploring Amazon's huge cloud system discovered 100 GB of **unsecured data** from a failed top-secret joint Army/NSA intelligence-sharing scheme. The government wasn't alone: the Republican National Committee left info on over 198 million **voters** in a publicly-open account there, too.

But Amazon is building a **supposedly secure cloud** just for the spies. Keeping it separate might preserve the data from all the **malware** and **botnets** infecting their cloud, which quickly became another irresistable target for hackers. Storing vital national security information up there will only make it more so.

However, it's not Amazon's most dubious idea. Their **Amazon Prime Air** drone delivery system might be. The packages would be supplied by **drone warehouses** floating overhead in blimps or nested in cell-phone towers. Not to worry, though, the drones will **self-destruct** in an emergency – no word yet about what might happen to the flying warehouses.

Amazon Air will drop packages by parachute to your home within full sight of neighborhood thieves, it will also **scan your property** to find opportunities to sell you even more goods and services.

If Amazon's that eager for your money, what happens once you let them into your house? The **Alexa** home assistant listens to conversations *all the time*. Not only that, due to a glitch, Amazon says, for a while Alexa **wouldn't answer** users who asked it if it was connected to the FBI or CIA. Now Alexa only says that it works for Amazon – how very reassuring.

Then there's the **Amazon Key** scheme where drivers actually enter homes to deliver stuff. Like the drone service, this is just for Prime members, but users will first have to purchase a cloud cam and smartlock kit from Amazon for $249 – plus disarm any home alarm system on days when deliveries are expected.

Remote users can also set it up to admit family, guests, maids, and dog-walkers. It didn't take long, however, for researchers to find out how to **hack the camera** so it freezes. Just like in countless TV hiests, viewers would see a closed door while the home is looted. Another hack leaves the door unlocked, too.

The **Internet of Things** includes many such devices that can be easily hacked. With little or no online security, they can become ideal hacker tools for building **gigantic botnets**. The latest one, **Reaper**, had assembled over 2 million devices, mainly unsecured webcams and open home routers, when it was detected just waiting to be used in an attack.

If such worries drive one to drink, Jim Beam offers a **smart decanter** for bourbon that will answer questions and pour booze on command. With only 6 months of connectivity, it's really more of a conversation piece, but it doesn't appear that any thought has been given to keeping it safe from kids or drunks.

The dolls are listening

Security concerns are important for toys that talk. A **European advisory**, however, warns that connected toys are insecure. Many can be hacked to allow strangers to listen and talk to your kids over the net.

Cloudpets also stored data openly on Amazon and **Furby Connect** has a number of flaws, too. But **My Friend Cayla** may be the worst. The doll collects personal data for analysis, and a nearby hacker could speak to the kids through its Bluetooth connection. The **FBI warned** parents but **German authorities** banned it, advising them to destroy the dolls.

Old-fashioned Barbies seem a lot safer by far.

Giving Safely, Effectively Online

As if gift-giving to friends and families wasn't expensive enough, it seems every charity has its hand out at this time of the year. And the need is enormous.

With devastating hurricanes Harvey, Irma, and Maria, major earthquakes in Mexico, vast wildfires across California, refugees from Myanmar and Syria, 2017 has had more than its fair share of disasters, both natural and manmade. Many people use the holidays and the end of the year as the time they give to those who need help, and many charities depend on it.

But donors deserve to have their hard-earned donations to go to where its most needed, not wasted in overhead, executive luxuries, or outright scams. With so many people begging on social media, how can you determine worthy from bogus causes?

If you've ever given anything online, signed a petition, responded to a survey, or signed up for an action alert, expect an unstoppable barrage of email solicitations from all quarters throughout the season.

Be wary of charities you've never heard of before, and if you do wish to respond to a plea, go directly to the concern's website to donate, rather than to click on a link in an email. Even before Katrina hit land, for instance, bogus Katrina websites were being set up. In the wake of the storm, the FBI found that over 4,000 fraudulent charity websites had been set up.

Beware of bogus sites pretending to be some real, well-known charity. Most non-profit websites end in **.org** not **.com**. Avoid any website ending in a series of numbers. Do not give out personal info. Don't send money overseas, delete any begging email that comes with an attachment, and be wary of anyone contacting you claiming to be a victim. Finally, don't hesitate to check out sites' reputations on Google.

If you want to give for one of the causes mentioned above, there's **Charity Navigator**. This non-profit site lists and rates a huge number of charities, and manages donations. You can easily split your gift up if you want to any number of organizations.

For local giving, **Great Nonprofits** does the same for various community groups across a range of causes to make for happier holidays for all.

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.