WESTON

So we should demand Congress index Social Security taxation to inflation, right? Based on the 1983 threshold numbers, that would ensure that only singles making over about $64,000 year, and couples making over $82,000 a year, would have to pay taxes on their Social Security income.

If only it were that simple.

The money collected from these taxes goes to two specific places: the Social Security and Medicare trust funds. Perhaps you're starting to see the problem.

Both trust funds are running short of cash and could be depleted in a few years. That doesn't mean they'll be bankrupt. It does mean they won't be able to pay 100 percent of promised benefits.

Social Security's retirement trust fund is expected to run dry in 2034, after which it would be able to pay only 75 percent of the benefits that have been promised. Yanking away what amounts to 4 percent of its revenue, which is what's generated by taxing up to 50 percent of benefits, would just hasten that day.

Medicare's hospital insurance trust fund is in worse shape. The fund, which pays for inpatient hospital visits, skilled nursing, home health care and hospice, is forecast to be depleted in 2026, just a few years from now. The money raised from taxing Social Security benefits makes up 8 percent of the revenue going into the fund.

So fixing the stealth tax will require fixing Social Security and Medicare as well.

Proposals to privatize or scrap these systems face strong political opposition. Plus, the proponents can't guarantee that future generations would be better off. Shoring up the current systems, by contrast, would ensure that today's workers get the benefits they've been promised.

That almost certainly means those of us who are still working will pay in one way or another. We could fix the problem virtually overnight by raising the Social Security tax rate by 1.415 percent to 7.615 percent and increasing the Medicare tax rate by 0.32 percent to 1.77 percent. (Employers would pay an equal amount, since payroll taxes are split between workers and employers.)

More likely, tax increases would be phased in over time and combined with other changes, such as raising the full retirement age and lifting or eliminating the current cap on how much of our earnings are taxed. (The current 6.2 percent Social Security tax applies only to the first $128,700 of annual earnings in 2018, while the 1.45 percent Medicare tax applies to all earnings.) You can experiment with possible solutions using the American Academy of Actuaries' Social Security Game.

Few of us are excited about paying more taxes, but shoving the burden onto retired people who've already paid their dues simply isn't right. Making the system more fair could benefit all of us, now and in the future.

DYSTOPIA

hosting of fake accounts for Russian propaganda.

It wasn't just Facebook. Google attracted concern about its continuous surveillance of users after The Associated Press reported it was tracking people's movements whether they like it or not.

It also faced internal dissent over its collaboration with the U.S. military to create drones with "computer vision" to help find battlefield targets and a secret proposal to launch a censored search engine in China. And it unveiled a remarkably human-like voice assistant that sounds so real that people on the other end of the phone didn't know they were talking to a computer.

Those and other concerns bubbled up in December as lawmakers grilled Google CEO Sundar Pichai at a congressional hearing — a sequel to similar public reckonings this year with Facebook CEO Mark Zuckerberg and other tech executives.

"It was necessary to convene this hearing because of the widening gap of distrust between technology companies and the American people," Republican House Majority Leader Kevin McCarthy said.

Internet pioneer Vint Cerf said he and other engineers never imagined their vision of a worldwide network of connected computers would morph 45 years later into a surveillance system that collects personal information or a propaganda machine that could sway elections.

"We were just trying to get it to work," recalled Cerf, who is now Google's chief internet evangelist. "But now that it's in the hands of the general public, there are people who ... want it to work in a way that obviously does harm, or benefits themselves, or disrupts the political system. So we are going to have to deal with that."

Contrary to futuristic fears of "super-intelligent" robots taking control, the real dangers of our tech era have crept in more prosaically — often in the form of tech innovations we welcomed for making life more convenient.

Part of experts' concern about the leap into connecting every home device to the internet and letting computers do our work is that the technology is still buggy and influenced by human errors and prejudices. Uber and Tesla were investigated for fatal self-driving car crashes in March, IBM came under scrutiny for working with New York City police to build a facial recognition system that can detect ethnicity, and Amazon took heat for supplying its own flawed facial recognition service to law enforcement agencies.

In some cases, opposition to the tech industry's rush to apply its newest innovations to questionable commercial uses has come from its own employees. Google workers helped scuttle the company's Pentagon drone contract, and workers at Amazon, Microsoft and Salesforce sought to cancel their companies' contracts to supply tech services to immigration authorities.

"It became obvious to a lot of people that the rhetoric of doing good and benefiting society and 'Don't be evil' was not what these companies were actually living up to," said Whittaker, who is also a research scientist at Google who founded its Open Research group.

At the same time, even some titans of technology have been sounding alarms. Prominent engineers and designers have increasingly spoken out about shielding children from the habit-forming tech products they helped create.

And then there's Microsoft President Brad Smith, who in December called for regulating facial recognition technology so that the "year 2024 doesn't look like a page" from George Orwell's "1984."

In a blog post and a Washington speech, Smith painted a bleak vision of all-seeing government surveillance systems forcing dissidents to hide in darkened rooms "to tap in code with hand signals on each other's arms."

To avoid such an Orwellian scenario, Smith advocates regulating technology so that anyone about to subject themselves to surveillance is properly notified. But privacy advocates argue that's not enough.

Such debates are already happening in states like Illinois, where a strict facial recognition law has faced tech industry challenges, and California, which in 2018 passed the nation's most far-reaching law to give consumers more control over their personal data. It takes effect in 2020.

The issue could find new attention in Congress next year as more Republicans warm up to the idea of basic online privacy regulations and the incoming Democratic House majority takes a more skeptical approach to tech firms that many liberal politicians once viewed as allies — and prolific campaign donors.

The "leave them alone" approach of the early internet era won't work anymore, said Rep. David Cicilline, a Rhode Island Democrat poised to take the helm of the House's antitrust subcommittee.

"We're seeing now some of the consequences of the abuses that can occur in these platforms if they remain unregulated without meaningful oversight or enforcement," Cicilline said.

Too much regulation may bring its own undesirable side effects, Cerf warned.

"It's funny in a way because this online environment was supposed to remove friction from our ability to transact," he said. "If in our desire, if not zeal, to protect people's privacy we throw sand in the gears of everything, we may end up with a very secure system that doesn't work very well."

IDAHO

records.

Its employees work to prevent threats like one that occurred in 2013, in which the Justice Department said seven Iranian hackers working at the behest of the Iranian government gained access to the controls of a dam in the suburbs of New York City. Prosecutors said the hackers would have been able to remotely access the dam's gate, but it was disconnected at the time for maintenance. Prosecutors in an indictment made public in 2016 called it a "frightening new frontier in cybercrime." The hackers remain wanted by the FBI.

The Dark Side room is in one of multiple buildings in Idaho Falls that house the lab's cybercore, a division within National and Homeland Security. It's decorated with workers' "alter egos," life-sized cardboard cutouts of "Star Wars" heroes and other famous characters such as Sheldon, the genius and socially inept main character of the comedy show "The Big Bang Theory."

"That workforce is a unique culture with brilliant minds," Cramer said.

The Idaho National Laboratory's cybersecurity also has an electronics lab to dismantle and examine computers, including pulling information off severely damaged storage drives. The electronics lab contains a map of the U.S. West's electric grid and a car-sized computer that helps test the security systems of Western utilities, including Idaho Power, which serves an estimated 1.2 million people in southern Idaho and eastern Oregon.

Brad Bowlin, an Idaho Power spokesman, said the company as a matter of policy doesn't comment on its cybersecurity efforts.

In general, hackers can include foreign entities and nation-states with sophisticated attacks, malicious computer geeks, and even kids with no intent to do harm but just a curiosity to see if they have the skills to breach a system's security. Those kids, it turns out, are candidates for the lab's Dark Side room.

"Those are the kids we're looking for," said Darren Stephens, a cyber-researcher at the lab.

The Idaho National Laboratory makes efforts to find them beginning with middle schoolers. It also looks for junior and high school students and has competitions that it plans to expand to nudge tech-savvy youths toward cybersecurity careers.

The lab recently held a contest among college students involving Idaho universities and other national labs and colleges where workers in the lab's Dark Side attempted to hack into systems the students tried to defend.

It's a fun competition, but it's also a proving ground to find the next generation of cybersecurity workers where a shortage of more than a million employees by 2020 is estimated. Cramer said the nation's universities don't even have curriculums to train future cybersecurity workers.

That's something he's working to change with Idaho universities that could ultimately offer degrees to draw those students and become a main supplier for good-paying jobs in cyber-security.

"The problem is so new and challenging that we don't have the workforce right now to challenge the problem efficiently," he said. "We're in a bit of a scramble mode to help get caught up and train folks to get our arms around a big national challenge."
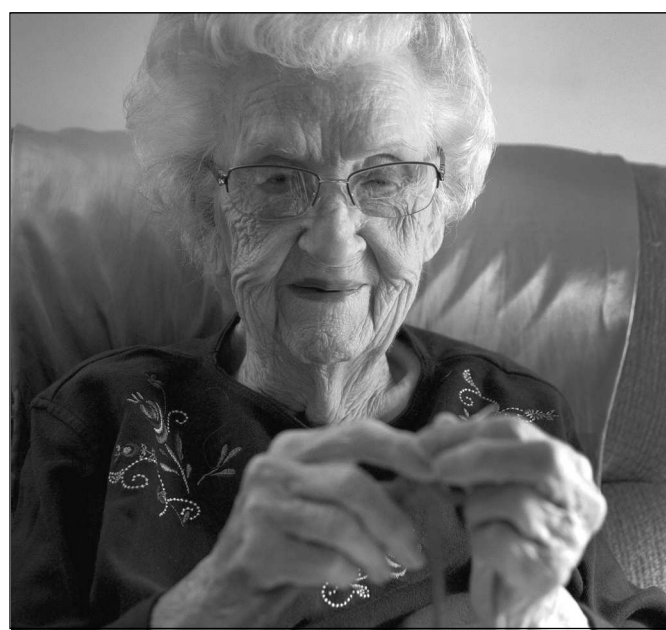
YARN

when the synthetic garments are washed.

Locally sourced yarn helps not only the environment but local businesses too, Parkes said. "There's the environmental impact of shipping goods all the way across the world and bringing it back, but now people are asking themselves, 'What if I can get the wool here and just keep it here?'"

McDermott echoed that sentiment: "Shopping local is allowing farmers to raise and keep their animals on the farm."

Consumer interest in locally sourced yarn inspired the Michigan Fiber Cooperative to produce a line, Fresh Water Fiber, which uses wool and alpaca from Michigan farms. It's processed by Stonehedge Fiber Mill and dyed by Why Knot Fibers in Traverse City.

One store that stocks Fresh Water Fiber is Wool & Honey in Cedar,

AP News photo

On her 104th birthday, Dody Patterson spends the morning knitting caps at her apartment at Good Samaritan Society Eugene Village in Eugene. In recent years, there's been a slow-growing demand for wool yarn that's completely produced in the United States

Michigan. Owner Melissa Kelenske said she buys from Michigan-based fiber artists and companies that focus on producing high-quality, ethically sourced yarn with attention to their environmental impact.

"I think the farm-to-table movement of eating local, shopping local — basically the major slow food movement — laid the ground work for the knitting industry," Kelenske said.

Another yarn company that supplies Wool & Honey is Brooklyn Tweed, of Portland, Oregon. Knitwear designer Jared Flood founded the company in 2010 to "preserve, support and sustain" American textile production by doing business with sheep farmers, fiber mills and dyers across the United States.

The business concept "was not so much about patriotism as supporting local economies," said Christina Rondepierre, Brooklyn Tweed's marketing manager.

"It was also the revitalization of East Coast mills and dyeing houses and the whole U.S. textile industry so they could sustain income and make sure towns and business were able to stay afoot," Rondepierre said. For example, the Harrisville, New Hampshire, Historic District mill village spins some of Brooklyn Tweed's yarns. The village was declared a National Historic Landmark in 1977.

But patriotism, too, is helping to revive the American wool industry.

After Ralph Lauren drew flak for making its Team USA apparel for the 2012 Summer Olympics in China, the fashion company had all Team USA apparel for the 2014 Winter Olympics made in the United States. The yarn used for the closing ceremony sweaters was 4,000 pounds of Shepherd's Wool from Stonehedge Fiber Mill.

McDermott was shocked when a Ralph Lauren representative asked her to supply the yarn.

"It was a mouth-dropped-open moment when I realized who I was talking to on the phone," she said. "It was a neat experience."