Opinion

BAKER CITY Herald
Serving Baker County since 1870

TUESDAY, MAY 18, 2021
Baker City, Oregon

Write a letter
news@bakercityherald.com

EDITORIAL

Another mess with the masks

It was good news, but like so much else during the pandemic, the CDC's announcement last week about fully vaccinated people doffing face masks and eschewing social distancing in most situations, indoors and outdoors, was also tinged with trouble.

The proclamation was if anything late in arriving.

After all, people who were fully vaccinated in, say, January were as thoroughly protected from COVID-19 then as those who were inoculated this month are today.

Nonetheless, the announcement by CDC Director Dr. Rochelle Walensky was a welcome reminder that people who are fully vaccinated get something much more important than a card and perhaps a sticker.

But this confirmation about the physical (and, indeed, emotional) benefits of vaccination from the highest level of the medical community was hardly a simple, happy milestone in states such as Oregon where mask requirements remain common.

Oregon Gov. Kate Brown and other state officials lauded the CDC announcement, to be sure.

But apparently it hadn't occurred to them that such a public statement was forthcoming, no matter that, thanks in considerable measure to growing vaccination rates, nationwide COVID-19 statistics, most notably the death rate, have been improving greatly.

Regardless, Oregon officials couldn't offer substantive advice to business owners about how to adjust to the CDC guidelines. Brown said the Oregon Health Authority would give new guidance soon. But that leaves business owners, many of whom have suffered greatly over the past 14 months, in yet another regulatory purgatory.

On Friday, May 14, Dr. Dean Sidelinger, the state epidemiologist, said businesses that allow customers to go without masks probably will be required to inspect customers' vaccination cards to ensure they are fully vaccinated.

This places an intolerable burden on business owners and their employees. Many have already had to endure tirades, and from both sides of the unfortunate "debate" over masks — from customers who consider mask mandates onerous and ineffective, and from those who berate businesses for failing to ensure that not so much as a square inch of inappropriate facial area is bared.

It's time for Oregon to allow businesses to set their own policies regarding masks, rather than continue to force them to risk losing customers over rules that were imposed upon the businesses.

That said, shoppers should respect the decisions that business owners make, and understand that some will continue to require masks.

That will annoy some customers. But should your personal disdain for wearing a mask for a brief period prevent you from patronizing a business whose products and services you enjoy?

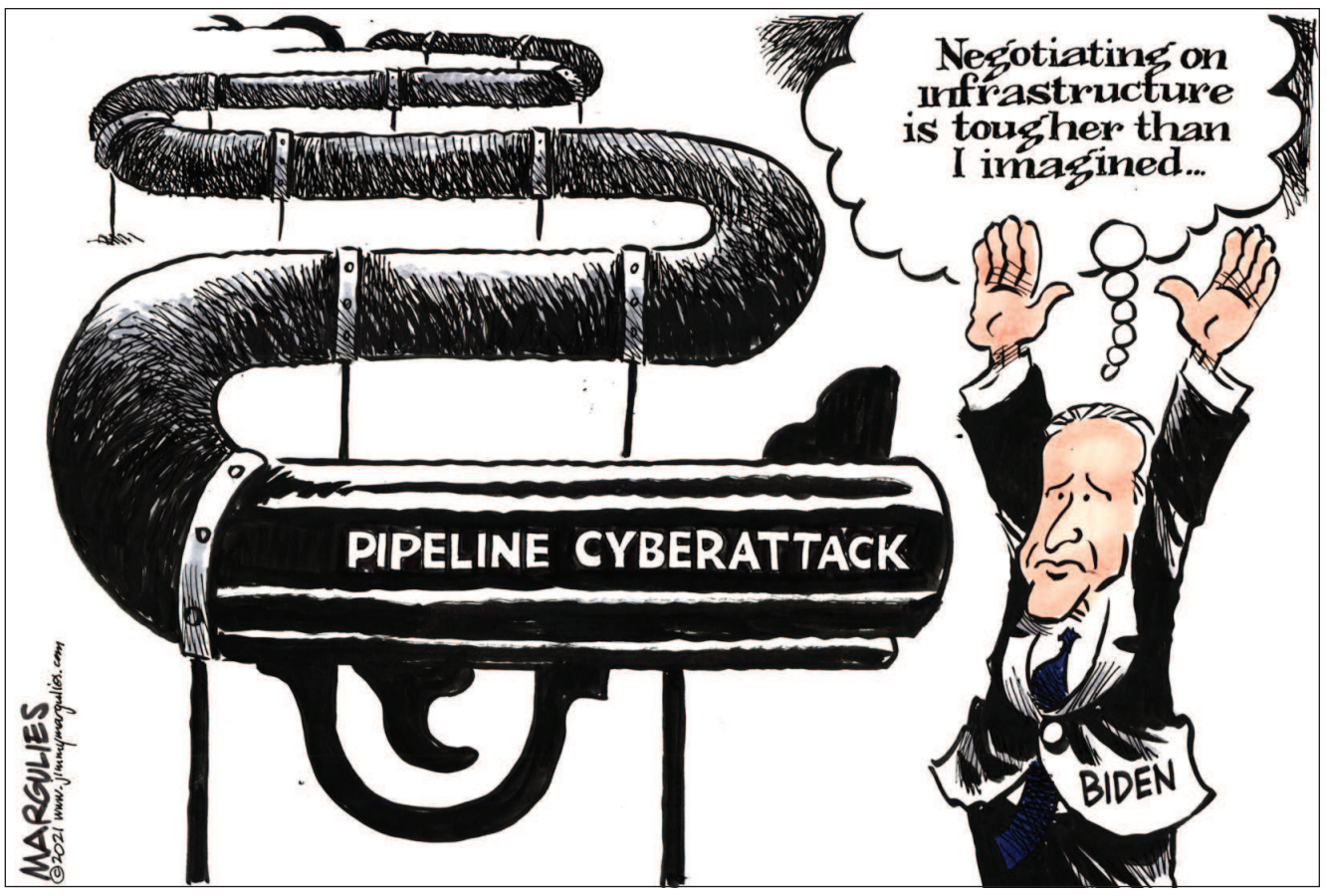
The cliché "we're all in this together" has enjoyed an unfortunate resurgence during the pandemic — unfortunate because it's such a misleading description of the situation. The reality, of course, is that COVID-19 has cracked open to yawning dimensions the divisions among us rather than pasted over them.

But when it comes to supporting businesses in a relatively small, relatively isolated community such as Baker County, we ought to be capable of setting aside something as trifling as a strip of cloth worn over the mouth and nose.

This pandemic will end; indeed, it clearly is on the wane. And when society returns to something we can all recognize as normal, we will want to be able to buy the items we've been accustomed to acquiring.

If wearing a mask for a few minutes in some of those businesses is the price to help that business survive these unprecedented times, then we should count that as a bargain and be happy to have it.

— Jayson Jacoby, Baker City Herald editor



Don't pay ransom to hackers

By Timothy L. O'Brien

Colonial Pipeline paid the ransom.

And after forking over $5 million to hackers who forced it to shut down an important fuel conduit, which spurred a bonkers run on local gas stations, the burglars gave Colonial a decryption key meant to sanitize its computer networks. But the tool didn't work very well. Bad trade.

Lesson: Don't pay the ransom.

Law enforcement authorities and other experts have been advising as much for years. Professional hostage negotiators regularly try to observe that maxim, too (though specialists who negotiate with terrorists have unusually complex dynamics to consider, and paying ransom may be the safest strategy for them).

When lives aren't directly at stake, the guidelines seem to be clear. Here's the Federal Bureau of Investigation's advice:

"The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illegal activities. Paying the ransom also does not guarantee that a victim's files will be recovered."

There's also a boomerang effect that arises when companies give bags of money to extortionists deploying ransomware. It seems to convince thieves that a target is an easy mark, and they will most likely circle back later and thump the same company or institution again. A particular willingness among U.S. companies to pay, combined with a porous and lackadaisical approach to cybersecurity in the private sector in America, may explain why the U.S. appears to draw a disproportionate amount of ransomware attacks in the developed world.

Hackers also may be shaking down U.S. companies more often simply because they're following the basic wisdom attributed to a bank robber, Willie Sutton: "Because that's where the money is."

Companies confronted with "double extortion" — the unhappy reality of having to pay hackers to unlock a digital network and then pay them again to recover stolen data — should remember that a significant portion of ransom-payers never get their data back anyway.

So what might an alternate approach look like? Consider Baltimore and Atlanta.

Atlanta got hit in 2018 when hackers asked for $51,000 in Bitcoin to revive municipal computers crippled as part of the broader GoldenEye attack. Atlanta refused to pay and chose, instead, to upgrade and secure its networks for $9.5 million.

Hackers laid siege to Baltimore's municipal computer networks in 2019 and demanded $76,000 in Bitcoin to go away. Mayor Jack Young told them to kiss off and then ate a $10 million fee to overhaul the city's networks and $8 million to write off unpaid taxes and other fees while computers were down. "We're not going to pay criminals for bad deeds," Young told the Baltimore Sun. "That's not going to happen."

There's a lot to be said for Young's perspective. A vulnerable network is going to need upgrades regardless of how ransom negotiations proceed, and there's no telling if paying a bribe will forestall all of the problems that come with a significant intrusion — so why not eat the costs upfront and move on?

Companies and other public and private institutions have many factors to juggle when hackers shake them down for money, of course. The Institute for Security and Technology, a private cybersecurity consortium, said in a recent report on ransomware that chief concerns include whether companies have cyber insurance policies and high-quality data backups. They also worry about the anticipated expense of paying for a prolonged system shutdown.

One obvious conclusion from that observation: All institutions in the digital era should have appropriate backups in place. That's not a complex fix. Also, companies should think about the expense associated with a shutdown the same way Atlanta and Baltimore did — proactively rather than reactively.

As for cyber insurance, well, that feels a lot like the disaster insurance that companies keep giving to homeowners who rebuild in flood and hurricane zones. Sure, it insulates against disaster, but it also encourages risk-taking. If an insurer is going to foot the bill for your ransomware payment, maybe you just find it easier to pay up rather than making your networks more resilient? That's certainly not lost on insurers. At least one top insurer, AXA S.A., is reportedly planning to stop underwriting new policies for that reason.

Companies and other institutions can avoid all of this by practicing good cyber hygiene in the first place, and they should bear that in mind when they demand that the federal government do a better job of protecting them from hackers. But once they've been burglarized, the last thing they should consider doing is paying off the burglars.

Timothy L. O'Brien is a senior columnist for Bloomberg Opinion.

OTHER VIEWS

Explain Trump's ban on Facebook

Editorial from The Pittsburgh Post-Gazette:

On Jan. 7, Facebook suspended President Donald Trump, striking a significant blow to his ability to communicate with the public. Banning him permanently from the platform would be a mistake.

An independent review board of activists, lawyers and journalists known as the Facebook Oversight Board has been considering the question of whether Trump's de facto ban was justified and whether he should be permanently excluded or allowed back on the platform. The oversight board has ruled that the original suspension was legitimate, but also that suspending him for an unspecified period is not.

This isn't a good outcome for free speech.

The remedy for bad speech is more speech, so the argument goes. And that adage holds true even when it's the president of the United States spouting falsehoods.

Facebook should post fact checks of Trump's content and remove posts that violate fair, clearly articulated standards. Banning Trump altogether goes too far. Trump, for better or worse, is a part of the debate. Because he says things that are false or controversial, it does not follow that his presence on this platform should be banned. This is a draconian reduction of free speech.

Facebook is a publishing platform, and an outsized publishing platform at that. It is a megaphone by which users can reach millions of people directly. The law has not yet caught up to social media giants, which never could have been anticipated by the Founding Fathers, and for now they remain largely unregulated. Publishers have a right and a duty, therefore, to curate and mediate the content that appears on their platforms. Facebook already employs independent fact checkers to help police this online forum for rule violations. Clearer rules and more and better self-policing are the way forward.

The former president's critics claim that the justification for his ban is that he incited an insurrection. Incitement of imminent lawless action is not protected by the First Amendment. The question of whether Trump violated that standard will play out in the judicial system, as it should. Social media companies should not mete out their own pre-emptive justice.

The Facebook Oversight Board did just that when it argued that Trump's initial suspension was justified because his posts "created an environment where a serious risk of violence was possible." There is no mechanism in Facebook's terms of use that suggest that someone should be permanently banned due to such language.

Moreover, if this is the standard that the company wishes to uphold, it should do so evenhandedly. The Black Lives Matter protests and riots of 2020 also were fomented by politicians and journalists, none of whom faced similar banishment. A specific, fairly enforced standard would help quell those arguing that Facebook's curation and fact-checking is biased on partisan lines.

The oversight board ducked the ultimate decision of whether to permanently ban Trump and called on Facebook to decide over the next six months whether to restore his account, make the suspension permanent or suspend him for a specific period of time.

This means there is still opportunity for the company to do the right thing and allow Trump back on the platform. His posts should be fact-checked and held to account. But the man himself should not be banned. He should be able to speak.