

Published in the April 3, 2017 issue of the New American magazine. Vol. 33, No. 07



Inside Track

Is Facebook Permitting Pedophilia and Child Porn on Its Platform?

While Facebook facilitates facial recognition and vacuums up user data by the exabyte, it draws the line at being asked to clamp down on child porn being passed around on its servers.

In a shocking story putting the massive social network in a very seedy light, Gizmodo reported on March 7, "When BBC journalists discovered child porn on the network and sent those images to Facebook last week, the company reported the BBC to police in the UK for the distribution of illegal images."

Investigative reporters from the BBC have a long history of tracking down the perverts that seem to pervade the Internet. After discovering that there was a significant amount of such images floating around Facebook, the network notified executives at the company, offering to sit down and show Facebook's representatives the evidence of pedophilia collected by BBC reporters, which Facebook requested.

BBC sent the images to the company, and then, almost unbelievably, Facebook backed out of the scheduled sit-down and reported the BBC to the police! In explanation of its extraordinary actions, Facebook issued a statement explaining, "It is against the law for anyone to distribute images of child exploitation."

Facebook says it is sufficiently policing child pornography and pedophilia by providing a "Report Button" on the site whereby users can identify potential pedophiles and "nudity and other sexually suggestive content." But BBC used the report button to alert the company to 100 images that appeared to break its guidelines. Only 18 were removed.

Facebook's rules also forbid convicted sex offenders from having accounts. But BBC found five convicted pedophiles with profiles, and reported them to Facebook via its own system. None of them were taken down.

Why would Facebook and its executives and managers permit such perversion on its site, a site accessed by over one billion people every day? A better, more relevant question would be why conservatives, Christians, and others of strong moral character continue to patronize a company so reluctant to run perverts off its site.

United Nations Pushes "HeForShe" Dolls for Boys

The United Nations has joined forces with a new company to push dolls for boys so your child can get in touch with his "feminine side."

Wrote PR Newswire on March 6, "HeForShe, UN Women's global solidarity movement for gender equality has teamed up with start-up company ... Boy Story to launch two special edition action dolls named Billy and Mason. The action dolls challenges [sic] current prejudice surrounding boys playing with dolls, and promotes the notion that both boys and girls should have the same opportunity to bond with a special playmate, and that all children, regardless of their gender, need to learn nurturing, emotional intelligence, and empathy."







Created by Boy Story founders Kristen Johnson and Katie Jarvis, Mason is a "Caucasian/Hispanic doll," while Billy is "African American." The company espouses the principles "How we play can change the world" and "Harmful stereotypes start young."

Boy Story's website states, "Girls should know that dolls are for everyone" and "Boys should know they can have dolls that look like them. They can learn to nurture, relate, and develop emotional intelligence." At 18" tall, Mason and Billy represent children who can walk and talk. Wouldn't nurturing be better encouraged if they were infants, requiring bottle feeding and diaper changes?

Boy Story writes, "Kids know and love diversity. When it comes to differences, kids really don't care much." So children love "diversity," which is defined by differences, but also don't care about differences?

Each Boy Story doll comes with an associated storybook, which likely doesn't involve Mason hunting with his dad or Billy going out for the football team. Then again, you never know. Explaining why the dolls are made in China, the company states that it needed to make them "both unique and very durable to hold up to all the rumbling and tumbling that boys tend to do." The special-edition version will cost you \$102 — on sale. Note, it doesn't appear the dolls are offered low-cost or no-cost in hardship cases so that poor boys won't be denied feminization.

Restaurants Add "Labor Surcharge" to Cover Minimum-wage Increases

Instead of increasing their menu prices in response to increased minimum-wage levels, restaurant owners are burying their increased labor costs at the bottom of each tab, the Wall Street Journal noted March 9. The increase, between three and four percent, only comes after the customer has completed his meal. The increase also increases the tip customers leave behind, as most customers leave a gratuity based on the check's total. This is going to raise the average customer's check, which has already increased by nearly 11 percent since 2012, close to five or six percent.

Some restaurant and fast-food store owners aren't burying the increase but are instead calling attention to it so that customers know that they're the ones actually bearing the brunt of the forced increase in the minimum wage. Sami Ladeki, the owner of six Sammy's Woodfired Pizza & Grill restaurants in San Diego and eight others across California, used to call it a "California mandate," but removed it after getting a call from the city attorney. Ladeki, who says he makes a profit of around one percent charging \$12 to \$14 a pizza, told the Journal: "This is not sustainable. People are not going to pay \$15 or \$20 for a pizza."

David Cohn owns 15 restaurants in San Diego and put in the surcharge, saying, "We want people to understand there is a cost. How do we stay in business with margins shrinking and competition increasing?"

The answer: automation. Late last year McDonald's announced that every one of its 14,000 stores nationwide will be replacing cashiers with automated touch-screen kiosks, starting with its stores where high minimum-wage laws were already in place.

The reality is that rising minimum wages increase unemployment and poverty and make it even more difficult for small business owners to remain profitable. Those owners won't be hiring new people, but







instead will ask more from their existing employees. They will be asking their workers to extend their hours or take a cut in benefits, or else be faced with the need to terminate them.

Dozens of Unvaccinated Students Banned From Class

Dozens of schoolchildren were banned from attending class in Rochester, Minnesota, on March 1 for not proving they received government-mandated vaccines. The reported number of students removed from school began at around 80, declining to 68 by the end of the day. The only alternative to the mandatory vaccines for schoolchildren is for their parents to jump through legal hoops to obtain an exemption. The controversial measure was largely effective in ensuring widespread compliance with the vaccine mandates, but critics are sounding the alarm about the threat to freedom and medical ethics.

Among the myriad shots now being required by state officials in Minnesota is one for chicken pox, which experts have questioned or even lambasted as counterproductive. Also required is the measles vaccine, which, according to the federal government's own data, is far more likely to kill American children than the disease it purports to protect against. Failure to receive even one of the more than one dozen mandatory shots resulted in the children being removed from class, according to press reports. Like most state governments across America, Minnesota authorities take their cues on vaccines from federal "recommendations" developed by the U.S. Centers for Disease Control (CDC).

For parents concerned about increasingly disastrous "education" and moral instruction in schools, along with the government's usurpation of power over their children's healthcare decisions, there is a growing range of options, including homeschooling. As Big Pharma and the politicians doing its bidding step up their attacks on parental rights and informed consent, the backlash is certain to grow, and that means more options will likely be forthcoming for concerned parents. Still, doctors and health experts urge parents to be well informed on risks and benefits before making important medical decisions for their children.

Good News From CIA Leak: Encryption Works!

With WikiLeaks' recent disclosure of the CIA's secret hacking program, many are left wondering how deep the rabbit hole goes. How secure are the devices and softwares that people all over the world use and depend on every day? While the mainstream media have reported on this as if either there is nothing to it or it's the end of both privacy and encryption, the truth is that encryption can still be used effectively to protect privacy.

As The New American has reported online in several articles, the tools (read: cyber weapons) developed by the CIA are scarily invasive. Any hacker who is worth his weight in silicon — and who also has access to these tools — has the ability to remotely access and control devices such as computers, mobile devices, and SmartTVs, to watch and listen to targets, as well as the theoretical (if not actual) ability to hack and control cars and trucks to disable or override steering, brakes, acceleration, and airbag controls. And thanks to the haphazard way the cyber-weapon files and documents were circulated within the CIA and its contractor companies, that could be a lot of hackers.

And despite the pooh-poohing by the intelligence community and many in the mainstream media, recent statements by the CIA and White House, coupled with the FBI's investigation into the source of the leaked CIA documents, serve as admissions that the disclosures are genuine. So regarding both the existence of the cyber weapons and the fact that the CIA lost control of them, it is really as bad as it







looks. But that is also very good news.

Buried in the CIA documents (and WikiLeaks' analysis of those documents) is the fact that there has been a shift in the way the surveillance state gathers information. In the wake of the Snowden revelations about mass surveillance almost four years ago, many — this writer included — began to implement ways to protect themselves against mass surveillance. The most effective tool for that is encryption. By encrypting data at rest (files and folders stored on a device), the owners of that data can be assured that it can only be accessed by someone with the encryption key or password. By encrypting data in motion (communications), the parties to those communications have the same assurances.

Reports of recent revelations about the CIA hacking program focus on the fact that the vulnerabilities exploited by the CIA-developed cyber weapons allow the hackers to compromise the underlying operating systems (such as iOS, Android, Windows, MacOS, Linux, Solaris, and others) to capture the data before it is encrypted.

So, how is that good news? Put simply: It means that encryption works!

The surveillance state has had to change its game, going back to targeting individual devices rather than casting a broad surveillance net and spying on everyone.

The take-away? Encryption works. At least for those willing to take the time and effort to make sure their endpoint devices (computers, mobile devices, routers, etc) are running up-to-date, reliable, trustworthy operating systems and software (which almost certainly excludes Microsoft Windows).

The answer to the question "How can people protect themselves from surveillance?" has not changed. Replace Windows with either Mac or (even better) Linux. Use open-source software and avoid proprietary software as much as you can. Encrypt everything you can, including your hard drive. Encrypt all communications, and encourage others to do the same. It's simple to do with applications such as ProtonMail and Signal. Keep your operating system and other software up to date. Don't store anything to an online backup service without first encrypting it. And — most importantly — think about privacy and security. Make it a guiding principle in the way you use computers. Any chain is only as strong as its weakest link. As for making a SmartTV secure, the best bet is to get rid of it. Period. The software is proprietary and the thing is designed as a spy tool.

Encryption has changed the game for the surveillance hawks. Now, instead of being able to conduct mass surveillance on scale, they are forced to compromise select and specific endpoint devices. If you are the specific target of a three-letter-agency, there is little you can do to avoid being spied on. For the rest of us, things are actually looking better.







Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



Subscribe

What's Included?

24 Issues Per Year
Optional Print Edition
Digital Edition Access
Exclusive Subscriber Content
Audio provided for all articles
Unlimited access to past issues
Coming Soon! Ad FREE
60-Day money back guarantee!
Cancel anytime.