Bitcoin’s Unsung Hero: Jeff Garzik

Will O'Brien

The Consumer Drone Age Has Arrived

John Meyer

The Unintended Consequences of Drug Regulation & Subsidies

John Meyer

The Tipping Point

Mackenzie Evans

EMP, the Most Frightening thing You’ve Never Heard of

John Meyer
1 Looking Back

2 Buckle Your Seatbelt:  
The Consumer Drone Age Has Arrived and This Flight May Have Some Turbulence

4 The Unintended Consequences of Drug Regulation

5 Something Isn’t Always Better Than Nothing

7 Student Loan Debt

9 Freeze Criminals out of your Credit Line

10 Bitcoin’s Unsung Hero: Jeff Garzik

12 The Tipping Point

14 Data Collection by Facebook and Google

16 Preventing Cancer with the HPV Vaccination

18 EMP, the Most Frightening thing You’ve Never Heard of

21 The Space Race:  
From Mansions to Micro-Apartments

---

Table of Contents

Bulletin • Winter 2015

Consumers’ Research is an independent educational organization whose mission is to increase the knowledge and understanding of issues, policies, products, and services of concern to consumers and to promote the freedom to act on that knowledge and understanding.

Consumers’ Research believes that the cost, quality, availability, and variety of goods and services used or desired by American consumers—from both the private and public sectors—are improved by greater consumer knowledge and freedom.

Executive Director: Joseph Colangelo  
Editor-in-Chief: Kyle Burgess  
Art Director: Mike Costelloe  
Staff Writers: Ethica Burt, Alec Engber, Mackenzie Evans  
Contributor: Will O’Brien  
Illustrations: Mike Costelloe

Copyright © 2015 Consumers’ Research. All rights reserved.

Consumers’ Research  
1801 F St NW, Washington, DC 20006  
202-898-0459
Looking Back

Products and Consumer Affairs Then and Now

In early issues of our magazine, we published a section called The Consumers’ Observation Post, which featured brief insights, speculations, and helpful tidbits on consumer goods, services, trends, and tools. Here we reexamine some of those snippets from January 1976.

Cruising for Ship Health Reports

Thinking of taking a cruise in the coming months? Afraid the ship you are considering might be a cesspit of unsanitary conditions? This is not an uncommon fear and is one consumers have had for a long time; however, there are ways to be better informed before making your travel plans. In January 1976, CR reported that cruise ship health reports are available to the public and detail health inspector findings. Over time, little has changed about the nature of the reports. They continue to be performed on a semiannual basis on ships that have foreign itineraries and carry more than 13 passengers.

One major difference is that in 1976 consumers had to write the then Department of Health, Education and Welfare in order to request the reports. They are now accessible online at the Centers for Disease Control (CDC)’s website. The grading scale is on a 100-point basis with a score of 85 or lower considered failing. Reports are sorted both by specific ships and by the cruise line they sail under. Consumers can also find reports on major outbreaks that occur. Today’s odds of boarding a contaminated ship are low, as out of the hundreds of cruises in 2015, only 10 reported a major outbreak.

Steering into Clarity

Also in 1976, CR wrote a tip clarifying what is meant by the age-old emergency driving advice of turning into the direction you are skidding. In the tip we quoted the American Automobile Association (AAA) as advising that when a vehicle’s rear end is skidding the driver should turn in the direction the rear end is going. Apparently discontent with this explanation, the current AAA brochure on winter driving advises you to “steer in the direction you want to go.” AAA also gives the same “steer in the direction you want to go” advice for front wheel skids, which have become more common as front and all-wheel drive automobiles continue to become more popular among consumers. Another important piece of advice when controlling a car in a skid is to lay off the brakes, as “slamming the brakes will only further upset a vehicle’s balance and make it harder to regain control.”

Other safety tips provided by AAA are to avoid using cruise control when driving on slippery surfaces (this includes ice, as well as water and sand). If at all possible, AAA advises not using your parking brake when it is cold out and making sure your gas tank is at least half-full to avoid gas line freezes. Most importantly, remember: drive slower, give cars more space, and keep in mind that stopping distance on ice can vary depending on the temperature (the stopping distance needed on ice at 0˚F is twice that needed at 32˚F).

Under the UV Lights

In our January 1976 issue, we warned about some of the hidden dangers of using UV lamps to get a tan. In particular, we warned of how excessive use can lead to burns, how mirrors can inadvertently lead to others getting tanned by accident, and the potential harm that can befall one’s eyesight should one attempt to read or watch TV under a sun lamp. Since then a multi-billion dollar industry has grown around tanning salons, but some of the same dangers remain. The FDA regulates the length of exposure time consumers can spend in a tanning bed so as to avoid burns and lower the risk of developing skin cancer; goggles should also be worn to prevent snow-blindness.

Studies have shown that children and adolescents are more biologically vulnerable to the risks of artificial tanning and the FDA and several pediatric associations have asked lawmakers to pass legislation prohibiting the use of tanning beds and booths by people under the age of 18. Some states, such as California and Texas, have already enacted such laws, while other states require parental permission.

Though fewer people use UV lamps for self-tanning, many use sun lamps to treat a number of skin conditions such as psoriasis, acne vulgaris, eczema and neonatal jaundice. They can also be used to treat circadian rhythm disorders such as seasonal affective disorder and delayed sleep phase disorder. ◄
Buckle Your Seatbelt: The Consumer Drone Age Has Arrived and This Flight May Have Some Turbulence

Will O'Brien

Whether you call them drones, quadcopters, or unmanned aerial vehicles (UAVs), expect to see more flying cameras buzzing around parks, cities, and every site you can imagine. Drones are one of the most popular tech gadgets on the market.

In this article written by guest expert Will O’Brien, Consumers Research takes a look at the drone phenomenon, and describes some of the challenges and opportunities this emerging industry faces.

Let's Define 'Drones'
The term “drone” has become the household word that refers to an unmanned aerial vehicle (UAV), either remotely piloted or autonomous. Drones can be big, like the ones used by the military, or small, like the consumer drones sold on Amazon.com, which now has nearly 2,500 quadcopters listed in its online store.

In the last few years, the major manufacturers of consumer drones, such as Chinese firm DJI or former WIRED editor Chris Anderson’s company 3D Robotics, have come down the learning curve in the key technologies used to stabilize flight and remotely pilot their aircrafts, making drones extremely simple to fly. At the same time, the prices of drones have plummeted as a result of competition, open-source innovations, and low-cost manufacturing. There are quality drones that sell for less than $100, and even the prosumer drones that have high-end cameras and advanced flight-control technology that cost only a few thousand dollars.

In short, drone technology is ready for the mainstream and drones are selling.

What can you do with a drone? You can fly it with a remote that looks much like an Xbox or PlayStation® game controller. It is a fun activity to simply race around the air with a drone. Most drones automatically hover in the sky when you take your hands off the controls, so you don’t have to be an expert pilot to use a drone.

Also, most drones come equipped with cameras, allowing you to easily capture aerial photography and video. Want to film the outside of your house to show off on a real estate listing? Or film a wedding from the sky? Or fly over a river or a canyon? Drones now enable consumers to capture footage that was previously only possible by professionals with expensive equipment.

Sounds Like A Great Innovation and Good Pricing for Consumers. What Could Go Wrong?
What could be bad about letting millions of drones into the airspace? Unfortunately, there are significant risks that need to be managed, and there have already been a number of close calls and a few accidents.

For example, in June, a man in Seattle was filming a parade and accidentally crashed his drone into a building. The drone spiraled down and hit a woman in the head, knocking her unconscious. The man was later charged with reckless endangerment.

Drones have been flown onto the lawn of the White House and have crashed into landmarks. During the California forest fire season, amateur drone pilots hoping to get some exciting footage caused delays for first responders who were hesitant to fly their aircrafts carrying water and fire retardant over the sites for fear of mid-air collisions. The Federal Aviation Administration (FAA) reports that drones have nearly collided with commercial airliners hundreds of times.

These risks clearly call for a set of rules around the usage of drones. So where are we with the development and implementation of those rules?

Rules of the Sky and Some Confusion
There are already basic rules in place for flying consumer drones. You must stay below 400 feet and at least 5 miles from an airport. There are also “no fly zones,” both temporary and permanent, such as national parks and sensitive sites (i.e. airports, prisons, power plants, etc.).

Many consumer drones now come with built-in GPS or geofencing features, which prevent them from flying into sensitive airspaces. Additionally, there are mobile apps that can tell you whether you are clear to fly based on your location, however most people don’t learn these rules until they first make a mistake. Because drones are so easily purchased online or at retail stores and there is no licensing or certification process to fly, you can be ignorant to the rules and cause a major problem by flying in the path of a jet airplane or helicopter.
In the FAA Modernization and Reform Act of 2012, Congress set deadlines for the FAA to define the requirements and process for keeping the consumer and commercial usage of drones safe, but the FAA has failed to fully implement such measures and has missed some deadlines.

The FAA recently announced that a federal law, which came into effect December 21, 2015, requires all unmanned aircraft to be registered to the owner by name, address, and model details. That way, if an accident or incident were to occur, police could track down the responsible party. The registration fee is $5, but will be waved for anyone who registers prior to January 20, 2016. Additionally, the FAA states that the fines for failing to register drones include civil penalties up to $27,500 and criminal penalties up to $250,000 and imprisonment up to 3 years.

Even with an established set of guidelines and proper usage, drone operators can get into trouble just from confusion. As a case study, consider Cleveland Aerial Media (CAM), a leading provider of aerial imagery, which was hired to film the demolition of a bridge near downtown Cleveland. The project was sponsored by the Ohio Department of Transportation (ODOT), which provided permission to CAM to film the explosion. After footage was published by CAM, viewers began filing complaints to the FAA about CAM violating temporary flight restrictions (TFR). Although ODOT had given permission, the FAA had issued a TFR for the same site.

After a meeting with the FAA, the confusion was cleared and CAM was given the greenlight to continue operating its business. Further, CAM was granted a Section 333 exemption, which gives the company broad permissions to fly where amateur pilots cannot, and to fly for commercial purposes.

In reflecting on the confusion, Cleveland Aerial co-owner Anthony Serio commented, “What we really need are a set of rules to make sure people fly safely, a way to enforce those rules, a proper way of tracking drones and holding operators accountable, and perhaps most importantly, a way for these small aircraft to communicate with other larger aircraft.”

Looking Ahead: Great Opportunities and Near-Term Challenges
The future is undoubtedly one full of drones. Amazon and Google have announced plans to use drones for delivery. Drones can be used to bring medication or first response equipment faster than ambulances. Drones are being used by journalists to fly into humanitarian crises to expose crimes and dangerous situations through raw video footage. Drones will be used across industries including construction, surveillance, security, real estate, television and film, wildlife management, agriculture, environmental monitoring, and search and rescue. And of course, consumer drones make for a fun way to capture a family holiday or event in your city.

But the future with drones needs to be one that is safe and respects the privacy of individuals. Just like when smartphones came out, consumers suddenly had amazing new technology at their fingertips that could take photos, give location-based directions, and connect to anyone over the Internet. And that same technology was initially scary because people were justifiably worried about inappropriate photo capture, stalking based on location, and mobile data companies breaching consumer privacy by peeking into their phone usage.

If we get this right, drones could add a lot of value and enjoyment to our daily lives. The challenge is that we could get it wrong in two ways. The first is to not have the right rules in place that protect consumers, and that is where we are today. The second is to have a set of rules that creates too much of an onerous burden on consumers who simply want to fly their $100 gadget they received for Christmas.

The solutions will come, as always, from the market. Drone manufacturers are already allowing app developers to build on top of their platforms. With more entrepreneurs working on solving these problems, the concerns of the FAA and other agencies around the world will largely be met, consumers will be informed and protected through smart software, and the drone market should continue to take off to clear skies. ▶

About the author: Will O’Brien is serial tech entrepreneur and investor. Drones is one of his top categories for disruptive innovation. Find him on Twitter at @willobrien.
The Unintended Consequences of Drug Regulation

All regulation and subsidy programs are prone to unintended secondary or indirect effects on the cost and availability of products. These secondary effects can be particularly acute in the highly regulated and heavily subsidized market for drugs. Two examples, one of regulation and one of subsidy, are presented below.

Retroactive FDA Review Causes Huge Price Increases
The idea of the U.S. Food and Drug Administration (FDA) going back to do safety and efficacy testing on grandfathered old remedies that have been on the market prior to modern FDA testing sounds good. However, this FDA program, which began in 2006 as the “unapproved drugs initiative,” has had the massive side effect of suddenly making many old, inexpensive generic drugs very expensive.

One egregious example of such price spikes is that Colchicine, an ancient gout remedy used for over 2,000 years, used to cost about 25 cents per pill in the U.S. Then, in 2010, its price suddenly jumped to around $10 per pill, a forty-fold increase. The mechanism of this price spike was that the FDA allowed URL Pharma, Inc. (bought in 2012 by Takeda Pharmaceutical Company Ltd.) the exclusive right to market Colcrys, its branded version of Colchicine. Then the FDA pushed the old versions of Colchicine off the market through what it called “risk based management.” Although the FDA usually grants only a three-to-seven year exclusive right to produce an approved version of an old drug, the patent for Colcrys will last until 2028 preventing competitors from producing the approved version as a generic drug until then. Colchicine is only one example of massive price increases resulting from this FDA program. The price of vasopressin, a drug used in cases of cardiac arrest, has risen ten-fold and a vial of neostigmine, a drug used to reverse the effects of anesthesia, has jumped eighteen-fold from under $5 to $90.

This FDA program may have made some old drugs a bit safer or established that an alternative is slightly more effective, but these generics had been on the market for a very long time without significant problems. Although the FDA’s program was supposed to focus on old drugs that had significant reports of safety or efficacy issues, the program has not been well-targeted and, in many cases, the drugs selected for study were not the ones that had problems. The FDA’s mandate focuses on safety and effectiveness and it does not take price into account when regulating a drug; consequently, it has given no consideration to the price effects of its initiative.

Consumers who were using inexpensive generic drugs that are reviewed under this program are likely to have to pay a lot more or try to find another alternative that the FDA hasn’t yet reviewed, or one that the FDA approved long enough ago that generic competition is again allowed and has had time to drive the price down. And even if consumers are successful in finding such an alternative, the replacement may be less effective, or in some cases, have an adverse side-effect for these particular patients.

Subsidy programs to help low-income patients may have unexpected pricing side-effects on other consumers
Many drug companies have “patient assistance programs” to aid uninsured or low-income patients in paying for expensive drugs. These programs sound well-intentioned and do help some people. On the other hand, they are not necessarily created for altruistic reasons or even for public relations, but sometimes to promote new drugs that are more expensive and not always better than the old drug(s) used for a particular medical condition.

These programs would not seem to affect anyone except their recipients, but they do have two secondary and indirect effects that can increase costs for unsubsidized consumers. The first and more immediate effect is that, because the money used for these patient assistance programs has to come from somewhere, the company may raise the regular market price a bit to make up the cost. The second and less apparent indirect effect is that patient assistance programs may steer people to costlier drugs and the cost increases may be surprisingly large.

Often, there is a reasonably priced drug, maybe at $50 to $100, that is considered to be the safest and most effective course of treatment for a particular condition. But, these programs may promote a new drug costing ten times as much and provide it at no cost to the patient.

The result of establishing the new, more expensive drug as a regular treatment is that insurance, either via an employer or a government program, will usually have to pay the extra cost. Then, in future years, premiums will rise to cover the cost for private programs, and taxes will increase to cover the cost for government programs. This is a variation on a more general phenomenon that, when a subsidy program is created to make a product cheaper or free for some, it either results in the price of that product rising for others, or everyone having to pay for the subsidy through fees or taxes.

Both of these programs appear to have the best of intentions—ensuring consumer safety and assisting consumers in need—however, without looking at the big picture and long-term, overarching effects, we fail to see the harm they actually cause.
The U.S. Food and Drug Administration (FDA) approved flibanserin (brand name Addyi) in August, and the product hit the market in November. Initially designed to treat depression, flibanserin obtained approval as a therapy for low sexual drive in premenopausal women, referred to medically as hypoactive sexual desire disorder (HSDD) – a treatment and disorder that have both been widely criticized as unsubstantiated.

Until now, there were no FDA-approved treatments for sexual desire disorders in men or women, in part, because none have passed the benefit-to-risk analysis considered by the FDA in its approval process, but also because sexual desire is complex, capricious, and does not lend itself to being treated with a single medication or course of therapy.

It’s easy for groups to attack or champion flibanserin based on whether HSDD is a truly unmet medical need. Proponents argue that low sexual desire is a distressing and emotionally painful disorder that warrants medical treatment. They also frame the discussion as a women’s rights issue, praising flibanserin as the first female equivalent of Viagra and the 26 FDA-approved medications to treat erectile dysfunction (ED).

Opponents argue that classifying low sexual desire as a disorder medicalizes or even pathologizes normal variation in sexuality. Furthermore, they counter Viagra-equivalent claims by making the distinction that ED medications treat the physiological barriers to achieving an erection in males who experience sexual desire, but cannot act on those desires due to insufficient blood flow; whereas, flibanserin interferes with neuropathways (like an anti-depressant) with the aim of increasing sexual desire in otherwise physically healthy premenopausal women.

Approaching the drug’s validity from this perspective is unhelpful and will result in impasse. The true point of debate lies solely with the FDA’s mandate and whether it followed that mandate. The primary objective of the FDA in drug approval is to determine whether the benefits provided by a proposed treatment outweigh the risks of that treatment. Using this framework, the existence or lack of other treatments for HSDD should not have had a disproportionately high influence on the decision. Ultimately, if a drug provides marginal or unclear benefits accompanied by risks which more than offset those benefits, the FDA should not approve it. Despite lacking sufficient efficacy to justify the risks, the FDA approved flibanserin without giving proper consideration to its principal directive.

Ignoring the drug’s opponents and granting the premise that there is an unmet need in the treatment of HSDD, flibanserin does not sufficiently meet that need in light of its risks and the FDA should have decided on that alone. Just as it is undesirable for regulators to overreach their authority and interfere where they have no mandate, it is undesirable for them to overlook their mandate and not interfere because “something is better than nothing.” If that something is more harmful than it is helpful, it is not better than nothing.

According the FDA, “Across the three trials, about 10 percent more Addyi-treated patients than placebo-treated patients reported meaningful improvements in satisfying sexual events, sexual desire or distress.” Two of these three trials resulted in the drug’s rejection by the FDA, with the most recent trial providing the “meaningful” support for the drug’s efficacy. This 10 percent improvement translates to an increase of roughly one additional satisfactory sexual event per month (with no baseline for differences among the sexual partners of trial subjects). Meaningful, indeed. (Certainly, there’s nothing safer – a glass of wine, for instance – that could achieve similar results.)

Trial results indicate that women receiving the recommended dose of flibanserin experience increased incidences of adverse effects including dizziness, drowsiness and nausea (11%:2-3%, trial:placebo); central nervous system depression such as fatigue, somnolence, and sedation (nearly 21% of trial group, three times greater than that of placebo group); hypotension and fainting without warning (especially when alcohol and certain medications are used); and in some cases appendicitis (6:0, trial:placebo). Furthermore, results on whether there is an increased risk of breast cancer resulting from the use of this drug are unclear.
“Because of a potentially serious interaction with alcohol, treatment with Addyi will only be available through certified health care professionals and certified pharmacies,” said Janet Woodcock, M.D., director of the FDA’s Center for Drug Evaluation and Research (CDER). “Patients and prescribers should fully understand the risks associated with the use of Addyi before considering treatment.” Even with training and certification, health practitioners routinely prescribe medications to treat symptoms those medications are not approved for – another risks the FDA should have taken into account before approving a daily medication that acts on processes of the brain.

When weighed against the risks (e.g. potentially fainting while driving or developing breast cancer), the benefits seem vastly outweighed, yet the FDA ruled otherwise. While the unintended consequences of this drug’s approval are yet unknown, FDA regulators may regret this decision when the first fatal accident occurs as a result of the use of this medication, as prescribed or otherwise. Of course, if the drug’s paltry sales since its launch are any indicator of its demand and long-run use, consumers are making wiser choices than the FDA.
The U.S. Department of Education recently confirmed that it will cancel the nearly $28 million of federal student loan debt incurred by attendees of the now defunct for-profit education chain Corinthian Colleges Inc. This is great news for the 1,300 students defrauded by Corinthian, which filed for bankruptcy in May. Not long before the company’s filing, the Obama Administration had announced that it would study whether to expand bankruptcy options for “all student loan borrowers.” Days after the Administration’s announcement, the Fairness for Struggling Students Act of 2015 was introduced in the Senate. A Congressional Research Service summary of the bill says it, “Revises federal bankruptcy law with respect to the exemption from the exception to discharge in bankruptcy for certain educational loans if excepting such debt from discharge would impose an undue hardship on the debtor and debtor’s dependents.” Over nine months have passed since the bill’s introduction and there has been no movement on the legislation.

Student loan debt has ballooned by more than 200 percent since 2007 to become the second greatest source of American household debt after home mortgages. Outstanding student loan balances now total more than $1.3 trillion dollars and almost a quarter of borrowers no longer in school have fallen behind on payments. The administration’s bankruptcy proposal would likely only apply to privately held debt, which accounts for a mere 10 percent of student debt nationally; the remainder is held by the federal government. The announcement came as federal agencies had been expanding programs that lower students’ monthly payments and eventually forgive some debt for borrowers in good standing.

Currently, there are very tight restrictions on the expungement of student loan debt through bankruptcy. Generally, a debtor must prove “undue hardship” by satisfying three criteria:

1. The debtor cannot maintain, based on current income and expenses, a “minimal” standard of living for the debtor and the debtor’s dependents if forced to repay the student loans;
2. Additional circumstances exist indicating that this state of affairs is likely to persist for a significant portion of the repayment period of the student loans;
3. The debtor has made a good faith efforts to repay the loans.

If these criteria are met, then the student loan is canceled and the remaining balance expunged. Creditors are not permitted to perform collection actions until the proceedings are completed, or until the court grants permission to do so. Lenders have argued that easing these restrictions would lead to higher borrowing costs for everyone due to the greater risk lenders would have to take on. In response to the bankruptcy proposal, the Consumer Bankers Association, the industry’s main trade group, said in a statement that less than 3 percent of borrowers with private student loans are in “financial distress.”

However, an April 2015 report by the Federal Reserve Bank of New York titled Student Loan Borrowing and Repayment Trends, 2015 paints a far less positive image of the financial circumstances of student loan borrowers. The report found that in the fourth quarter of fiscal year 2014, more than a third of graduates of four-year institutions with outstanding loans faced an increasing loan balance despite always having been current on payments. Meanwhile, 20 percent of borrowers were current but had previously fallen behind, and another 17 percent were either delinquent or in default. Only 29 percent of borrowers were both current on payments and seeing decreasing loan balances. A separate report by the nonpartisan Institute for College Access and Success found that between 1993 and 2012, the average debt load for graduates of four-year institutions climbed from $9,450 to $29,400.

These data clearly demonstrate that our present student lending system is unsustainable over the long-term. To be sure, student loans are a necessary means of expanding educational opportunity to those who would not otherwise be able to afford college. But the loans themselves must ultimately be repayable for this to hold true, and thus allowing student loans to be discharged in bankruptcy does nothing to address the underlying issue of affordability. In order to find an appropriate solution, it is necessary to first examine the various factors contributing to the explosion in student loan debt.
While greater levels of student lending can be a reflection of higher rates of college enrollment, the New York Fed report concludes that increases in the number of borrowers and loan amounts have grown at rates roughly three times faster than enrollment. This suggests that present levels of student debt are primarily a result of students needing to borrow more money to pay for postsecondary education, and that higher postsecondary enrollment was an important but less significant contributing factor.

This explanation is further supported by the immense increases in postsecondary tuition over the past 30 years. Between the 1982-83 and 2012-13 enrollment years, average tuition at public institutions increased nearly 54 percent in inflation-adjusted dollars. Tuition at private nonprofit and for-profit institutions grew by more than 52 percent over the same period.

A Cornell University report by Ronald Ehrenberg, Ph.D. found that one important contributor to the declining affordability of higher education is federal policy. The Justice Department used antitrust regulations to end collusion among elite institutions with regard to the allocation of financial aid. The schools had previously agreed to primarily distribute aid based on financial need, but the termination of this agreement has helped to fuel the growing use of expensive merit-based aid packages as institutions vie for the most accomplished students. Meanwhile, the value of federal grants to lower-income students has not kept pace with inflation, driving institutions to make up the difference by raising tuition further.

The report found that tuition growth is primarily a result of the “arms race” among colleges and universities to attract the most qualified students. Ehrenberg’s report stated that in order to keep up with competitors, colleges must constantly spend more to improve research, faculty, education, facilities, and instructional technology. At the same time, parents and students want to purchase the “best” education possible. High-scoring students have increasingly decided to enroll in selective (read “expensive”) private institutions, and the gap in pay between those who graduate from these schools and other graduates has increased substantially over the past 30 years. Rather than reduce costs or reallocate funds, universities have largely chosen instead to spend more money. The growing importance of published college rankings, which include spending per student as one measure of educational quality, has served as a catalyst to this arms race.

One proposal put forth by the Obama administration would seek to slow the rate of tuition growth by ordering the Department of Education to rank colleges on educational outcomes, cost-effectiveness, spending per student, and other factors to measure the quality and cost-effectiveness of the education students receive. These rankings would be used to determine the amount of federal aid granted to each school. This plan came under intense criticism from higher education institutions, who argued that such rankings would be arbitrary and that tying federal aid to these would only further exacerbate the educational arms race that is primarily responsible for tuition growth in the first place.

In response to this backlash, the Department of Education abandoned the ranking system in favor of an information campaign to increase student awareness of the costs and outcomes of higher education. The Department offers College Scorecard (collegescorecard.ed.gov), an online resource where prospective students can look at information including graduation rates, annual cost, and average salaries, compared to national averages. While this resource does not provide the incentive structure of the previous plan, it does offer students an abundance of data to help them make an informed choice about higher education.

Unfortunately, the College Scorecard program alone is unlikely to significantly slow the rate of tuition growth and other measures must be taken if higher education is to become affordable for every student who merits enrollment. One proposal would cap loan payments at some proportion of borrowers’ pay (10 percent, for example) so that payments remain sustainable even if the education received does not provide a good career outcome. Others have argued in favor of a system in which student loans are forgiven after 10 years of on-time payments.

Yet another option would be to increase funding for federal aid programs, which has seen its real value decline substantially over the years. However, it is possible that this would give schools an excuse to raise tuition in proportion to the increased aid, so that cost of attendance increases and more or less negates the effect of greater funding. A possible solution to this would be to tie increased aid to College Scorecard data without “ranking” the institutions as the Administration had desired previously. In theory, this would provide an incentive for schools to improve educational outcomes without raising costs unnecessarily.

Regardless of the specifics, no policy alternative can solve America’s student loan crisis without addressing its root cause: skyrocketing tuition costs. ◄
Freeze Criminals out of your Credit Line

Kyle Burgess

If you use a credit card or share your date of birth or social security number to fill out forms or confirm your identity, you are vulnerable to risks such as identity theft, credit card transaction fraud, or even having lines of credit opened in your name. As demonstrated by all the recent cyber hacks, it’s nearly impossible to fully protect your identity and credit, given the prevalence of security breaches in commerce and even government activities involving personally identifying information (PII), such as birth dates, home addresses, telephone numbers, and social security numbers.

Typically, when financial account information, such as credit card information, is stolen, it can be replicated to make fraudulent purchases. However, something you may not be aware of is that fraudsters can use stolen PII to apply for and receive credit cards, loans, apartment leases, vehicle leases, mobile phone accounts, and anything else that requires a credit history check – all in your name! Compared to the slight inconvenience caused by having a current account hacked (i.e. notifying your bank or credit card company and getting a new card, usually with the fraudulent transactions covered by your financial institution), it may take you a over a month to resolve issues caused by someone using your PII to open a new account in your name. Unlike noticing transactions on your statement that you didn’t make or having the bank call you to notify you that your account was compromised, you often don’t know a fraudster has opened an account in your name until it’s too late and they have wreaked havoc on your credit score.

One thing consumers can do to protect themselves from this type of fraud is to implement a security freeze or credit freeze. “What’s that?” you ask. A credit freeze blocks third parties, such as leasing agents or credit card companies, from accessing your credit report. These third parties are usually looking at your credit history to determine the likelihood you’ll repay your debt if they give you a loan or lease you an apartment or car. If third parties cannot access your credit report, then they will not extend credit to you, or fraudsters posing as you. You can grant permission to unfreeze or “thaw” your credit report when you actually do wish to open a new line of credit and need to grant third parties access to your report.

To implement a credit freeze, you can call or go to the websites of the consumer credit bureaus (such as Equifax, Experian, TransUnion, and Innovis) and follow the instructions they provide. Depending on your home state, fees are roughly $10 per credit bureau.

According to a 2013 U.S. Department of Justice report, people “who had personal information used to open a new account or for other fraudulent purposes were more likely than victims of existing account fraud to experience financial, credit, and relationship problems and severe emotional distress.” This is likely due to the lengthy and involved process of resolving this type of fraud. Credit freezes aren’t free and the process can take a half-an-hour to set up; however, if you’re one of the unfortunate 50% of American adults whose PII has been exposed due to a hack, $30-$40 is a price you may be willing to pay for a little extra peace of mind and the potential headache and stress associated with new credit line fraud.

Why have I never heard of a credit freeze before, you ask? Well, it’s complicated. Businesses that issue credit want to ensure that consumers have easy access to credit. By doing so, they can generate revenue off that credit. Having consumers freeze their credit runs contrary to this interest, so they do not market credit freezes to consumers. Of course, credit issuers also have to deal with the cost of fraud, but presumably they believe that cost to be lower than the ubiquitous use of credit freezes. Financial institutions are regulated and have an obligation to protect consumer information, but those requirements only cover so much. Credit report companies generate revenue off credit reports, so they do not market credit freezes either. That leaves organizations like Consumers’ Research, which exist to serve consumers and give them the information they need to make informed decisions.

It is important to bear in mind that credit freezes do not protect you from other kinds of identity theft or credit fraud on existing accounts. You should always be careful with your PII, only sharing it when necessary with trusted parties. It is also a good idea to regularly monitor your credit and debit card statement activity. There are a number of other steps you can take, such as making sure that your browser is on a page with a verified security protocol, such as an SSL certificate, when purchasing items or services online. Lastly, don’t be afraid to say no when asked for your PII. We’ve gotten so used to reciting our birth dates and social security numbers whenever asked, that we forget to stop and think about whether those we’re interacting with truly need that information to conduct whatever activity we’re engaging in. You’re your own best advocate when it comes to safeguarding your PII.
For someone who spends his days building the future, Jeff Garzik is a pretty humble guy. In fact, you’d be forgiven for never having heard of him, even if – like a growing number of Americans – you use the products of his labor every single day. In an industry with no shortage of self-promotion and inflated egos, Garzik is an outlier, an unassuming presence in a sea of proselytizing tech ambassadors who are all exalting the future of money.

I’m talking, of course, about Bitcoin. Garzik, the overtly polite family man I met over burgers in Atlanta, Georgia, is one of the people in the world most responsible for making it happen and keeping it together.

Garzik is hard to pin down. The day we met, he had just gotten back from Abu Dhabi, where he spent the previous week meeting with sheikhs and UAE businessmen about Bitcoin and its ever more popular analog, the blockchain. Although we had met on a couple of occasions, I was struck, as always, by his modesty and humility.

Recently, Garzik has focused on the issues of scaling and security, looking for ways to safeguard mining nodes against attacks. After he briefly working to put with the bitcoin in space (his company, Dunvegan Space Systems, would have floated bitcoin nodes in satellites but failed to gain traction) he has formed his first large Bitcoin startup, Bloq, whose mission is currently described in generic terms as “professionalizing the entire Bitcoin ecosystem.”

Garzik has the best ratio of braggadocio to actual accomplishments in the Bitcoin community. That is, he has very little of the former, and a staggering amount of the latter. As one of the most prolific programmers to work with the open-source Bitcoin protocol, he has made over 1,000 “commits” to the system¹, and has served as one of the community’s most judicious voices since he got involved back in 2010. He’d be a great candidate for someone to make decisions for the entire Bitcoin ecosystem, unfortunately because the idea of a “king” of Bitcoin is antithetical to the ethos of open-source, he’s the last person who would accept such a position.

As he continued his self-education, he developed a fondness for open-source platforms like Linux. After graduating from Georgia Tech in 1996 he worked for CNN as one of their first web developers. He then returned to his open-source roots and worked at Redhat for the bulk of his career.

As someone who has questioned the Federal Reserve system along with current monetary policy, Garzik had seen a number of alternative digital currencies come and go and hadn’t put much stock in them. With Bitcoin, he says, the story was different. The open-source platform attracted his attention early on, and he started programming on it in 2010, less than a year after the protocol’s release.

Garzik’s refers to his first patch to the Bitcoin software as a “lesson learned” in open-source contribution. In 2010 he uploaded a patch that, if accepted by the bitcoin network, would have immediately changed the Bitcoin block size to 20 MB, the same transaction rate as Paypal. In hindsight, he admits that it was a very naïve patch, since it didn’t fully account for the idea of how patches are accepted or the incentives of miners. If only some people adopt the patch, Garzik, argued, “then some people are on Bitcoin island and some people are off Bitcoin island.”

He goes on to stress the importance of avoiding what he calls “incompatible laws.” Pointing out that open-source development and Bitcoin especially is all about merit, “As a developer, you have to prove yourself as new entrant in the marketplace of ideas and you don’t do it based on your words or your looks or your personality, it’s your code output.”

¹ A “commit” is a permanent change made to a computer system or piece of software. When Bitcoin was first introduced by the anonymous Satoshi Nakamoto in 2009, he allowed coding-adept users to propose changes, subject to approval of the community at large. After approval, the proposed change becomes a “commit.”
To scale or not to scale

The problem with electing a leader of Bitcoin is that if someone had the authority to make decisions for the network, it would open up that person to duress or corruption and all the problems that Bitcoin is trying to solve. As such, many of the developers are resistant to leadership. This in turn creates a governance problem, because if you don’t have any leadership, it’s very difficult to decide which direction to go in the block size debate. The “block size debate” is the current deliberation within the Bitcoin community on whether, and how, to increase the size of “blocks” that are processed by bitcoin miners. A small block size means fewer transactions can be processed at one time, but also requires less work by miners, the people who process bitcoin transactions. A larger block size means that Bitcoin can scale to the size and activity level of Paypal, Bank of America, or anything. Ultimately, the attempt with Scaling Bitcoin, which is a series of conferences that have already taken place in Montreal and Hong Kong, is to shine a light on the different viewpoints from different factions throughout the Bitcoin community. One of the main problems, Garzik points out, is that there’s no way to measure users of the system to get consensus. Who do people think should be in charge of making decisions about Bitcoin, and what does Jeff Garzik think of those decisions?

Developers? In Garzik’s opinion, “developers should not be economic high priests. You shouldn’t trust me to make decisions for Bitcoin.” How do you sample the economic consensus, then?

Large bitcoin holders? Garzik also thinks that’s the wrong way to go, giving large owners of bitcoin control over the direction of development. “That’s not egalitarian, and I want a far more egalitarian system as opposed to one that disadvantages new people coming in to the system while helping a small clique of stakeholders.”

All bitcoin users? Well, how do you sample bitcoin users? “This guy just owns a penny of bitcoin, should we trust him with as much power as someone who has invested a lot more into bitcoin? How well informed is this person? You see the same thing in democracy. Donald Trump is an excellent example of someone who has a lot of popular support,” says Garzik. “I’ve bought his books,” he continues, “and studied him for decades well before his presidential run. It’s very easy for a populist candidate to get a lot of support. Translating that back into the Bitcoin analogy, you don’t want mob rule to dictate where Bitcoin goes.”

“The best attempt at solving this problem is to be very public about what we’re doing as developers and soliciting input from key Bitcoin actors and as many users as we can,” says Garzik.

On the topic of governance, Garzik ends with one of his favorite truisms. “Democracy, like decentralized systems, is intentionally inefficient.” Centralized systems, he points out, can have single points of failure that can be exploited to take down the entire system. Decentralization adds friction to the system but at the same time creates resilience in the face of attack.

To continue the democracy analogy, Garzik believes that an ultimate system to govern Bitcoin will account for many of the diverse interests that bitcoin users, programmers, holders, and miners all represent. Working through Scaling Bitcoin, Garzik has helped to shape a governance model that will accommodate the interests of all stakeholders – whatever that ends up looking like.

What does Garzik think about the future? He’s wildly optimistic about the potential for technology to continue improving lives. With programmable money, consumers will have greater protection of their own assets than ever before. With the help of Moore’s Law, the cost of processing power will continue to decrease, putting the most sophisticated computing power in the palm of every consumer, all across the world.

He sees threats to this prosperity, of course. One of the threats that stands out in his mind is the current debate surrounding encryption, and the position of many government officials that encryption methods should only be permitted when “backdoors” are installed that afford law enforcement access to information that is otherwise encrypted. He points out that, from a programming point of view, it is both logically and mathematically impossible to have a backdoor that only the good guys can use. Combine that with the recent trend in which governments are not sharing the knowledge they have about exploits with institutions that are vulnerable to them, and the encryption backdoor presents a recipe for disaster.

Who is Jeff Garzik? He’s the son who carries his father’s dog tags with him as a reminder of the people who have worked hard to give him the opportunities he’s been given. He’s the programmer who once naively tried to change the Bitcoin block size and, years later, is trying to do it the right way. He’s the man who might save Bitcoin, and who won’t take any credit for it.
Can you name a multi-billion dollar expenditure of economic resources that American consumers voluntarily relinquish each year? Tips, of course. In the U.S. alone, 3 million servers and bartenders are economically dependent on the estimated $44 billion in annual tips they receive from their customers. Tips are expenses that U.S. consumers have the ability to avoid, yet frequently choose to undertake. What motivates this economically “irrational” behavior, and how do we decide the right amount to tip? Tipping has been shown as a cost-effective way for restaurant owners to motivate servers to provide quality service, but can it survive a possible increase in the federal tipped minimum wage and the onset of tablets at the table?

To Tip or Not To Tip

Although there are records of our Founding Fathers giving tips to their slaves, the practice of tipping servers did not become common in the United States until the early 1900s. Tips are now common in over thirty service occupations. Among workers that commonly receive tips are doormen, bartenders, masseuses, golf caddies, hair stylists, parking attendants, sports instructors, taxi drivers, and perhaps most commonly, servers.

Because tippers are free to pay whatever they want in exchange for services that have already been rendered, many economists view tipping as an “irrational” and “mysterious” behavior. By their logic, providing a tip is a deliberate and voluntary act of individual consumers that can only be explained by individual human motivation. Approximately 80 percent of U.S. consumers report that the desire to reward good service drives their own tipping behavior, and 70 percent report that a desire to help servers underlies their tipping. Other motives include the gain of social esteem, fulfilled obligation, and preferential future service. Restraining motivations are motivations that prevent people from tipping, such as the desire to keep tip money for other uses and the dislike of the status differences implied and created by tipping.

“Change” in the Weather

Whatever the underlying motivation, 99 percent of consumers do choose to tip their server for a meal at a full-service restaurant. But what factors affect the decision of just how much money to tip a server? In 1940, the standard tip size was only 10 percent. Today, the Emily Post Institute advises consumers to tip servers 20 percent of their bill, excluding tax, for very good service, 15 percent for adequate service, and no less than 10 percent for poor service.

Certain factors, both in and out of the server’s control, can affect the size of the tip customers choose to leave. Nonverbal behaviors such as smiling, a light touch on the shoulder, or squatting at eye level with a customer have been shown to increase tip size. Servers can also expect higher tips when they introduce themselves by name and compliment a customer’s choice of menu items. A number of outside factors that also have a positive effect on tip size include pleasant weather, desirable background music, and the restaurant’s location in an urban area.

The Great Wages Debate

The amount of the tip matters to tipped workers making the minimum tipped wage. Restaurant servers are almost three times as likely to fall under the federal poverty line. According to the Fair Labor Standards Act, the current tipped minimum wage is $2.13. Many people feel strongly about whether or not the U.S. government should raise the minimum wage, but what would a raise in the tipped minimum wage mean for the restaurant industry?

Some experts view an increase in the tipped minimum wage as an extension of the competitive model. This means that an increase in the tipped minimum wage would reduce the employment of workers eligible for tip credit and can either decrease or increase aggregate earnings of the affected workers depending on the elasticity of labor demand. This assumption ignores possible employee responses to an increase in the tipped minimum wage, which include tip pooling and requiring additional non-tipped work. In a competitive restaurant industry where the employer is unable to mitigate the effects of a higher tipped minimum wage, an increase in the tipped minimum wage drives up the cost of tipped workers and should have the same effect as an increase in the minimum wage—fewer hours of employment, an increase in hourly earnings, but an ambiguous effect on aggregate earnings in the industry.
Concerns about tipping continue to be cited as a primary reason why the custom should be abolished and replaced with inclusive pricing or automatic service charges. An increase in the tipped minimum wage may enhance an employer’s willingness to pay the cost of monitoring servers. Additionally, because the tipping method allows for servers to be tipped virtually any amount, an increase in the tipped minimum wage in an attempt to increase servers’ income may actually achieve the opposite result.

**Tablets at the Table**
Some restaurant owners are taking a different approach to serving patrons—installing iPads to replace waiters. The onset of tabletop and P.O.S. iPad systems is completely changing the way consumers tip. Major restaurant chains that have already installed tabletop tablets include Chili’s, Applebee’s, and Buffalo Wild Wings. Unit-servers remain on hand to bus tables, refill drinks, and fulfill requests.

Forty percent of consumers say they would pay the same tip in a tablet-equipped restaurant, but 45 percent say they would reduce their tip either a little (33 percent) or a lot (12 percent). Twenty-six percent of younger consumers, however, would actually increase their tip if they paid by tabletop tablet. As the role of the server evolves, it remains unclear how the practice of tipping will respond.

P.O.S. iPad systems often automatically adjust preset tipping options on orders less than $10 to either $1, $2, or $3. Even if they choose the $1 tip because they are in a hurry and the barista is staring at them from the other side of the counter, consumers could find themselves paying an over 40 percent tip on a $2.38 cup of coffee!

The very concept of tipping is evolving beyond the service industry with the rise of startups like ChangeTip that allow Internet users to tip each other using Bitcoin. Users of ChangeTip can give tips to reward other users for great content, talents, performances, and more using social networking sites like Twitter and Facebook. According to ChangeTip CEO Nick Sullivan, the platform boasts over 100,000 users that have collectively tipped $2.5 million. Could there be a time in the near future in which consumers are prompted with a “tip” button next to the “like” button on Facebook and Instagram?

**At Your Service**
Whether they do it to help others or to avoid feelings of guilt, American consumers surrender over $40 billion of wealth annually in the form of tips to various types of service workers. Next time you find yourself either armed with a pen and staring at the “gratuity” line or face-to-face with an iPad requesting a 40 percent tip, remember that you are individually responsible, in part, for the continuation of this puzzling American custom.
n the wake of revelations regarding National Security Agency (NSA) surveillance programs and the theft of personal data from the Office of Personnel Management (OPM) as well as from major retailers, much attention has been paid to the security of online communications and data. However, relatively little attention has been given to the data collection practices employed by online advertising companies such as Google and Facebook. By tracking users' online activities, scanning messages and emails, and collecting user passwords for other websites, Facebook and Google have been able to use the data collected through these aggressive practices in order to achieve and maintain market dominance in online advertising.

With over 1.44 billion active users communicating and sharing interests on Facebook, the social media company has compiled a vast store of data that are highly conducive to targeted advertising. However, the company has been aggressively expanding its data collection efforts beyond compiling the information users knowingly share with the public. For example, Facebook tracks the place and time of pictures uploaded to the site, and logs user location information to further target friend recommendations and advertising based on geolocation data.

News and video streaming websites often include a button to “like” or “share” a particular article on Facebook. It would likely come as a surprise to many that the company is notified whenever such pages are visited and by whom, regardless of whether the visitor clicks on either of the buttons. When a user logs into Facebook from a mobile device, the company automatically connects the device’s unique identification to that Facebook profile. The company’s Atlas advertising platform is then able to serve online ads based on that profile, even if the user is not logged in, while also compiling all of the websites visited on the device in order to further hone ad targeting. Atlas does not rely on cookies, which means there is little one can do to reduce the data collection. Facebook now allows users to opt-out of interest-based advertising on the Digital Advertising Alliance website, but this option notably does not allow users control over the amount or kind of data collected. It merely promises that the data companies collect will not be used to target advertising.

Facebook has come under fire from the Federal Trade Commission (FTC) for its privacy practices in the past. In 2011, the company settled charges with the Commission that it had violated its promise to users that it would keep their information private. Among the charges enumerated in the FTC complaint was that the social media company made changes to its website in 2009 that made public certain information, such as “friends lists,” that users had designated as “private,” without notification or consent. Facebook also falsely claimed that third-party applications would only receive data necessary for them to run, and that user data designated as “friends only” would only be shared with people on a user’s friends list, when in fact it was also shared with third-party apps. Facebook told users their data would not be shared with advertisers, but shared it anyway. The FTC settlement included a consent decree requiring the company to receive consent from users prior to any future changes in their privacy practice.

Google’s data collection is even more pervasive than that of Facebook, thanks to its diverse array of platforms and programs it can employ for this purpose. Google, like Facebook, scans the messages and emails sent to or from users of its Gmail e-mail service. Unlike Facebook, however, this practice is not limited to its own users, but also extends to senders and recipients with non-Google email accounts. Online search engine queries and the websites selected from search results are likewise compiled and analyzed. Google’s popular Chrome browser records all web pages a user visits unless the user manually turns this function off, and does not use the company’s “recommended” settings.

Google also has a long history of collecting passwords for wireless networks and online services by less-than-transparent means. For example, it was revealed in 2010 that Google’s “street view” cars included Wi-Fi receivers that were used to collect wireless data from surrounding networks. Google has admitted to collecting the MAC addresses (unique Wi-Fi hotspot device IDs), network SSIDs (network names assigned by users), and Wi-Fi transmission data (including online passwords and email content) from networks within range. The Federal Communications Commission (FCC) fined Google
$25,000 for obstructing its investigation into the matter, but the company was able to prevent the Commission from making a determination as to whether Google violated the Wiretap Act. A lawsuit regarding this issue filed by 38 states was eventually settled for $7 million.

In 2012, the FTC fined Google $22.5 million – the largest civil penalty it had ever handed out – for violating a 2011 consent decree issued by the Commission over privacy issues relating to its Buzz social media platform. Buzz, which has since been discontinued, allowed Gmail users to share photos, videos, and status updates with their contacts. Privacy concerns arose when users discovered that their email contacts were automatically added to their social network, prompting an FTC inquiry that resulted in a settlement barring the company from “future privacy misrepresentations,” requiring it to implement a comprehensive consumer privacy program, and subjecting it to “regular, independent privacy audits” for the following 20 years. Just one year later, the FTC found that Google had violated the previous settlement by misrepresenting its privacy policy to users of Apple Inc.’s Safari web browser. Google had told Safari users that their browser’s default settings automatically opted them out of having advertising cookies installed on their devices. While Safari’s default settings did in fact have this feature, Google purposefully bypassed the privacy software to install tracking cookies in spite of these protections.

A central issue with the practice of widespread data collection is that companies expose users to some degree of risk by storing so much of their personal information, and by the methods used in doing so. A September 2014 study by Experian found that 43 percent of companies experienced a data breach in the previous year, and that 60 percent had experienced a breach within the previous two years. It is simply impossible for Google and Facebook to guarantee that the data they collect will remain secure, and great financial harm could be done to millions of users if their vast stores of data were to be stolen. Additionally, the same unseen connections that the companies use to gather data can also be exploited by cybercriminals to steal personal information. Governments also regularly request data from both companies for use in ongoing criminal investigations, which raises important concerns regarding the civil liberties of users whose records are turned over and used as evidence in criminal proceedings. In effect, Google and Facebook can thereby be used as warrantless evidence-gathering tools for governments around the world and at home.

There is also evidence that the personal data being collected is not only used for targeted advertising, but also for personalizing prices for online goods and services. This takes two principal forms: price steering (manipulating the order of search results so that higher- or lower-priced items appear at the top of the list) and price discrimination (showing different consumers different prices for the same item on the same website). A Northeastern University study released in November 2014 measured the prevalence of these two practices on a variety of e-commerce and comparison shopping sites, while controlling for geolocation and other extraneous factors. While only one of the major retailers examined was found to engage in price personalization, comparison shopping sites such as Priceline and Expedia systematically employed both price steering and price discrimination in displaying search results. One travel site, for example, offered a particular hotel in Paris to one user for $565 per night, while the same hotel was offered to another user at a nightly price of $633. The report found that such variations amounted to “hundreds of dollars” in some cases.

Both Facebook and Google have tried of late to give the appearance of greater transparency with regard to their collection and handling of user data. However, their previous violations of consumer privacy – and the ever-present possibility that hackers or government agencies will acquire sensitive information as a result – are risks of which many Google and Facebook users are unaware. While recent polling has shown that consumers are concerned about the privacy of their personal data, the companies’ present market dominance will make any change difficult to achieve without a major paradigm shift among their users.
Editor’s Note: It has been six months since the Centers for Disease Control (CDC) recommended routine, universal vaccination against the human papillomavirus (HPV) starting as early as age 11. While the public debate on this topic has faded, the urgency of this issue has not. HPV vaccination levels have not risen significantly in recent years, limiting the rate at which HPV-associated cancers may be avoided.

Consumers’ Research is not in the business of telling parents how to parent, but we are in the business of providing consumers with the information they need to make educated decisions. This article is intended to serve as a fact sheet that approaches HPV as any virus with potentially fatal consequences. It focuses on the cancer risks caused by this extremely common virus and emphasizes the importance of seriously considering the virus, as one would do with any other harmful and preventable disease. The fact sheet explains how the virus is spread and how routine vaccination against the virus can be incorporated into existing recommended vaccination schedules for children.

Why children? Because children have the greatest chance of avoiding HPV-related cancers. The vaccination only protects against those HPV variants to which individuals have had no prior exposure.

According to the CDC, given the often undetected prevalence of the disease, exposure to one variant or another is an almost certain outcome, even among those who have partnered with only one person.

While no vaccines are perfect at disease prevention, and none are free from side-effects or rare complications, exposure to a cancer-causing disease is also not without the risk of severe consequences.

The Virus

Human papillomavirus, commonly referred to as HPV, includes over 150 types of different, but related, viruses. The virus is known to cause cancer of the cervix, vulva, vagina, penis, anus, and throat, and in some cases can cause genital warts. The strands of the virus known to cause cancer are different from those that cause genital warts. The virus is spread via intimate skin-to-skin contact, typically through sexual intercourse but also through non-penetrative sexual activity. For this reason, the virus is considered a sexually transmitted infection (STI). HPV is so common among men and women that the CDC estimates nearly all sexually active men and women contract a strand of HPV at some point in their lives.

According to the CDC:

• 79 million Americans are currently infected with HPV.
• 14 million people become newly infected in the U.S. each year.
• About 360,000 Americans contract genital warts each year.
• Approximately 12,000 women in the U.S. get cervical cancer each year.
• Each year approximately 4,000 women die from cervical cancer.

HPV Causes:

• 72% oropharyngeal cancers
• 63% penile cancers
• 69% vulvar cancers
• 75% vaginal cancers
• 91% of anal cancers

Strand 16 of the HPV virus (HPV 16) has been identified as a major cause of oropharyngeal cancer. This includes cancers of the throat, tongue, and tonsils. By 2020, HPV is expected to cause more cases of oropharyngeal cancers than cervical cancer.

The virus can be spread by both men and women who exhibit no symptoms of the virus. Anyone who is sexually active, even with just one partner, is at risk of contracting the virus. Symptoms often develop years after the virus is initially contracted, which may make it difficult to know one’s standing.

There is currently no way for a person to know his or her “HPV status” as there no approved test to detect HPV. There are HPV tests to screen for cervical cancer, but these tests are only recommended for women over the age of 30 and do not address strains of HPV-related cancers in the throat or mouth.

The Vaccine

While there is no HPV test, a preventative vaccine for the virus does exist. The HPV vaccine is a series of three shots over a 6-month period, including Cervarix, Gardasil, and Gardasil 9. All three of the shots protect against cancer. These vaccines are recommended for all children ages 11 to 12, as well as adults who have not received the vaccination up to age 21 for men, and 26 for women. The vaccination does not treat existing infections.
Cervarix: designed to prevent infection from HPV 16 and 18, which cause 70% of cervical cancers as well as most HPV-related genital and head and neck cancers.

Gardasil: designed to prevent HPV 6, 11, 16, and 18. HPV 6 and 11 are estimated to cause 90% of genital warts cases.

Gardasil 9: designed to prevent all strands covered by Gardasil, as well as 5 additional strands including 31, 33, 45, 52, and 58, which are also linked to cancer.

Low Vaccination Rates
Despite the above guidelines, vaccination rates for the virus remain much lower than the potential rates estimated by the CDC. According to a 2014 report published by the CDC, only 57.5% of girls and 34.6% of boys ages 13 to 17 in the U.S. had received the first dose of vaccination in 2013. While these rates represent a slight increase from the 2012 figures, they suggest a missed opportunity by physicians and parents to vaccinate their children. The CDC notes that if teens received the first HPV vaccination at the same time as their other required vaccines, the rate of vaccinations for 13-year-old girls would be approximately 91.3%.2

Why the Low Rates?
There are many reasons public health officials attribute to the below-desired rates of HPV vaccinations. Among them include:
• Framing the discussion of HPV as a discussion about STIs instead of one about cancer
• Lack of guidance from health care professionals due to discomfort discussing sexual behavior with children, a limited understanding of HPV-related cancers, and/or anticipated parental resistance.
• Lack of awareness that the HPV vaccine is available and recommended for aforementioned age ranges, as well as both males and females.
• Lack of knowledge of the number and types of cancers linked to HPV.
• Belief that getting the HPV vaccine will encourage children to become more sexually active.
• Belief that the child is too young to be sexually active and therefore does not need a vaccine to prevent an STI.
• Religious objections to the vaccine.
• Mistrust of the vaccine and concern it may cause autism or other harmful conditions.
• Lack of public financing – as the vaccine is not free, it may be perceived as an “extra” measure, rather than standard.

Fostering Understanding
To boost the HPV vaccination rates to their optimal estimated rates, the vaccine should be introduced as soon as the child is eligible at age 11, along with the other vaccinations required at this age such as the Influenza vaccine, Meningococcal Conjugate vaccine, and the Tetanus, Diphtheria, Pertussis (Tdap) vaccine. As a primary concern among parents is the perceived sexual nature of the virus, introducing the vaccine as one that ultimately prevents cancer, rather than an STI, is crucial. In addition to this, ensuring both physicians and parents are provided educational materials regarding HPV can ensure a higher understanding of the virus, its symptoms, and its effects on both men and women. Physicians should also be trained to talk to parents about the virus, including the sexual nature of it, so the conversation can be started as soon as a child is eligible for the vaccine. Ultimately, the decision to vaccinate one’s child is the choice of the parent. By having a strong understanding of the effects of HPV and its symptoms, physicians can have a more effective dialogue with parents regarding HPV and its link to cancer.

What Else Can You Do?
In addition to getting vaccinated, it is recommended that a person who is sexually active further protect their health by:
• Getting screened routinely for cervical cancer (women ages 21 to 65).4
• Use condoms correctly during intercourse. However, condoms may not fully cover the infect areas and therefore may not offer full protection.
• Be a part of a mutually monogamous relationship. ▶

Sources
So, what is an EMP?

An electromagnetic pulse (EMP) is a disturbance of the Earth's electromagnetic field that can affect all electronic equipment, including consumer and commercial goods and machinery with electronic components, but is not directly dangerous to people. Although some other minor categories exist, major EMP events are typically classified in two ways: EMPs caused by a high-altitude nuclear explosion and natural EMPs caused by a solar storm. A nuclear EMP has three components, known as E1, E2, and E3, but natural EMPs have only the E3 component, making it comparatively less severe, although likely more extensive and longer-lasting.

E1 is a freely propagating wave that strikes nearly instantaneously and lasts less than a second. It causes high-frequency “electromagnetic shock” to electronics and electronic systems over a very large area— in other words, it “fries” them. The usual protections against lightning and normal electrical surges are not sufficient to defend against an E1 EMP. Protection requires specialized technological hardening and if the E1 surge is intense enough, it may destroy even equipment with light specialized shielding and most consumer electronics. Furthermore, any device using an antenna is set up to accept electronic signals and cannot be shielded. Only specialized technology integrated into equipment can harden it against E1 EMPs. E1 also destroys supervisory control and data acquisition (SCADA) components that are essential components of many parts of the national infrastructure.

E2 is also nearly instantaneous, following E1 by a fraction of a second and affecting a somewhat larger area. It is a lower amplitude phenomenon having effects on electronics similar to a lightning strike. An E2 pulse would compound E1 damage, destroying many items surviving an E1 pulse, either because their protections were already damaged by an E1 pulse or because they are inherently more vulnerable to an E2 pulse.

E3 is a longer duration pulse, lasting up to one minute, that is not a freely propagating wave, but a result of electromagnetic distortion in the earth's atmosphere. E3 disrupts long electricity transmission lines and damages the electrical supply and distribution systems connected to these lines. E3 is particularly damaging to long-line infrastructure, such as electrical cables and transformers. An E3 pulse could do very widespread damage to the U.S. power grid, depending on its strength and geographic location.

What is the potential fallout of an EMP?

While a solar storm can cause temporary disruption of broadcast and satellite communications and damage satellites, its most dangerous aspect is ionized plasma particles moving at a much slower speed that cause a “geomagnetic storm” producing E3 EMP effects at or near ground level. Current solar storm forecasting provides 12-18 hours to a few days’ warning of these plasma particles. The risk of severe effects is much greater at high latitudes and drops off at lower latitudes, especially below 40 degrees north. The warning time would allow the adoption of many mitigating measures to protect power plants and prepare for electrical supply interruptions. Nevertheless, a severe natural EMP would likely cause blackouts that could last weeks or months, because its effects do not simply collapse the grid, but also destroy critical components necessary for its restart and functioning.

Most of us have experienced a blackout, at least locally, as a result of severe storms and many a longer one, as with Hurricane Sandy. But the effects of an EMP-caused blackout would be more pervasive and prolonged, even for entities with backup power, such as hospitals, that usually have reserves good for hours or a few days. Light, heat, water, banking, communications, the Internet, sanitation and medical services would all be affected. Cell phones would work, until their charge or battery is exhausted or until cell phone towers’ backup power is exhausted. Many motor vehicles would not be initially affected, but fuel supply would be difficult. Trains would be immediately affected, as most are electric-powered and track control and switching equipment is electric. The effects of a natural EMP event would be exacerbated if it occurred in the winter, as cold would be an immediate threat to health and life. The magnitude of the disaster would depend critically on the ability to maintain civil order and bring in fuel for transportation and generators to keep some critical centers minimally functional.
A nuclear EMP would cause all the effects of a natural EMP and many other damaging effects. Its E1 and E2 components would destroy the actual electronics in many kinds of equipment and machinery. A major additional obstacle to recovery would likely result from damage to or destruction of electronic components of power plants that would render them inoperable; and in many instances actual physical damage would result from the consequent loss or inoperability of control mechanisms. Largely because there is no actual experience with such E1 and E2 pulses, there is a considerable range of opinion as to the percentage of destruction and as to how much protection equipment would receive if it is turned off or even unplugged and/or disconnected at the time. There also is disagreement among experts as to what percentage of motor vehicles would be inoperable because of the destruction of their electronic components, but many, especially older models with fewer electronics, would survive.

How likely is a severe EMP event?
The August 28-September 2, 1859 “Carrington Event” was the most intense solar storm in modern times, but it did little damage to a pre-electric economy. The general consensus is that a Carrington-level event strikes Earth about every 150 years, but one could occur at any time or not for many years. Although such solar storms are rare, one similar to the Carrington Event did narrowly miss Earth on July 23, 2012. The worst actual solar storm in recent times caused the Quebec black out of 1989, an event similar to the New York City and Northeast black out of 1965 or the Northeast blackout of 2003 (non-EMP caused events).

While the likelihood of a natural EMP event is subject to some level of scientific prediction, this is not true for a nuclear EMP attack which depends on the capabilities and decisions of nuclear nations. An effective EMP attack requires nuclear weapons and missile systems able to deliver them at a high altitude above the United States. The intensity of the E1 and E2 EMP is proportional to the square root of the size of the explosion, so moderate kiloton-level explosions do nearly as much damage as larger ones. The area of the serious EMP is proportional to the height at which the explosion occurs, as the propagation of E1 and E2 EMP is line-of-sight. Such an attack does not require many or large nuclear explosions. Even one such explosion at the relatively low yield of 30 kilotons at a height of only 20 miles above Pittsburgh would affect the entire Northeast and much of the Midwest and Border States. Three or four such explosions in the proper pattern or one explosion centrally placed at a greater height, such as 100 miles, would hit most of the United States.

Such an attack would cause great and lasting damage, probably the worst that America has ever experienced. While there are a range of opinions on the likelihood of this threat, most observers consider the major threat to be from irresponsible nuclear or near nuclear powers such as North Korea and Iran. While Iran is not yet nuclear and North Korea does not have an ICBM, an attack could be launched from a ship offshore with a missile as unsophisticated as a Scud.

What actions are being considered or have been taken?
The most comprehensive review of the threat has been the 2008 Report of the Commission to Assess the Threat to the United States from EMP Attack – which also considers the dangers from a natural EMP. Since its publication, no comprehensive plans have been developed and no extensive programs have been initiated to protect civilian infrastructure against either EMP threat (the military is extensively protected).

The Federal Energy Regulatory Commission (FERC), the most directly responsible federal agency has worked with the North American Electric Reliability Corporation (NERC), an electric industry group, in developing new electricity reliability standards which were adopted October 16, 2014. Some of the resulting improvements marginally increase survivability in an EMP event, but they are generally considered not to be effective against a major natural or nuclear EMP event. FERC has not adopted or even proposed a comprehensive plan specifically directed toward protecting against the natural EMP danger. On July 22, 2015, the Government Accountability Office (GAO) issued GAO Report 15-692T in which it reviewed all EMP efforts nationally and noted some good initiatives, but found that no overall program exists to effectively mitigate an EMP attack; it did note the existence of useful research and development, such as the RecX project to produce more survivable transformers.

Legislation, known as the SHIELD Act, was proposed and passed the U.S. House in 2014 requiring industry and government to promulgate and implement standards and processes to address the electric grid’s current vulnerabilities to a natural EMP, but the bill died in the Senate and has not advanced in either House this session. This year, the House Oversight and Government Reform Committee’s subcommittees on National Security and Interior held a May 23rd hearing on the EMP threat, and the full committee held a hearing on July 22nd as did the Senate Homeland Security Committee on the same day. However, neither the SHIELD Act nor any other EMP legislation has advanced in either House this year.

Costs are a critical consideration in any EMP protection effort. Unless upgrades are done as a crash program, these costs could be spread over several years and incorporated into currently scheduled infrastructure upgrades. Estimates vary as to the cost to protect key components of the electric grid, such as high-energy transformers,
from a natural EMP well enough to prevent a long-term catastrophic blackout. The range is from about $2-6 billion, with the higher numbers looking more credible, because a set of systems needs protection and damage to any one of them could greatly retard recovery. Protecting separate natural gas systems would be less expensive, likely costing under $1 billion. These measures would, in the general opinion of experts, greatly mitigate the results of any such natural EMP.

Discussion of EMPs often does not differentiate between threats from weapon-generated EMPs without use of nuclear technology (not addressed in this article), the serious threat of a natural E3 EMP, and the even more serious threat of a nuclear EMP with E1, E2, and E3 pulses and little or no warning time. Credible protection against a nuclear EMP is much more expensive, which explains some of the controversy that exists between those who say the job can be done relatively cheaply and those who say it is much more expensive.

For protection against nuclear EMPs, the most expensive component is the protection of power stations from E1 and E2 surges, with one estimate at $23 billion for that component alone, and an estimated total price tag of $30 billion over five years for a program to protect all major power systems. An additional possible protection against a nuclear EMP that could defeat such an attack entirely would be extension of the current antimissile system to protect the whole country. Existing technology would be used, adding an East Coast base, already under consideration, to the existing Alaskan base and adding radar installations to monitor the southern approaches to the United States – also, existing Aegis missile defense navy ships could be reassigned to protect the southern approaches to the United States.

The decision on EMP protection is analogous to a business or consumer decision on what risks to insure and how much insurance to carry. Currently, we as a society are essentially uninsured against both natural and nuclear EMP risks. The decisions we face are which of them are likely and/or dangerous enough to require such insurance, what technological fixes are available and how much we are willing to spend. One consideration to keep in mind is that complete protection is neither technically nor financially possible; protective measures under discussion aim to protect key components, mitigate damage and make recovery feasible.
For decades, American consumers have been vying for more space. The U.S. Census Bureau reported that by 2007 the average size of a single-family home increased from 1,645 square feet in 1975 to a peak of 2,520 square feet. Though the construction of large homes continues, a new wave of urbanism has triggered the emergence of a rising trend, which contradicts the notion that “bigger is better.” That trend? Micro-apartments.

What are micro-apartments?
Micro-apartments represent a form of housing comprised of less than 400 square feet of living space. Typically, these units are designed to address the increase in single-person households taking place across major cities. Developers and city planners have begun to embrace this form of living as a way to maximize profit per square foot and help manage urban density. In turn, residents find the new micro-apartments meet their demands for affordable, prime-location homes.

The Millennial Shift
At present, the Millennial Generation (defined as individuals born between 1980 and 2000) is growing up and moving into cities – searching for smaller, cheaper living quarters in urban settings. In many cases, the convenience of vicinity has drawn twenty-somethings to city life. The influx of Millennials into cities has resulted in high demand for single-person units. Developers and city planners have begun to embrace this form of living as a way to maximize profit per square foot and help manage urban density. In turn, residents find the new micro-apartments meet their demands for affordable, prime-location homes.

Crediting Credit
The 2007 housing bubble burst and subsequent recession resulted in a reassessment of risk in the housing market, forcing many homebuyers to look for spaces that required smaller investments and less risk in the long run. Homebuyers reevaluated the worth of big-ticket items, becoming more conscious of their wallets and the value gained from major purchases. In the suburbs, home prices became unfeasible for many city-workers affected by the recession, pushing them to the city to rent efficiencies and save money. With central city housing consisting of less than 50 percent homeownership, renting instead of owning a residence alleviates the stress of risky investments.

The Energy Wallet
The trend of living smaller is not without energy conservation perks in terms of cost-cutting. Smaller homes mean less energy usage and thus less money squandered. Opower, a software and data collection company, reports that the largest 1 percent of homes use over four times as much electricity as the average family home. A 1,600 square foot home uses approximately 9,500 kilowatt-hours (KwH) per year. In turn, the largest 10 percent of homes (6,400 square feet) use 2.5 times more electricity (roughly 24,000 Kwh) per year. Conversely, the energy usage of a micro-apartment is about 2,360 KwH. Less energy used means more money saved, furthering the appeal of smaller living to Millennials and those with post-recession mindsets.

Will less space continue to grow as a trend? As long as this wave of “New Urbanism” continues, affordable prime-location abodes will continue to be in demand. Census numbers predict that at current rates, single households will make up the largest category of households, likely driven by this urbanizing generation. Christopher Leinberger of The Brookings Institution notes that developers profit as well, “A bit cheaper for the renter — yet more profitable per square foot.” Housing shortages in large cities like New York become apparent when looking at the numbers; the city has 1.8 million households with 2 or fewer people but only 1 million studio and one-bedroom apartments. As cities continue to grow, saving doesn’t seem like a trend that will soon fade.