ISSUE GUIDE • UPDATED EDITION, 2013

NATIONAL ISSUES FORUMS
www.nifi.org

>>What Should Go on the Internet?

Privacy, Freedom, and Security Online

THE INTERNET IS an integral part of American life in the 21st century. What began in the 1960s as a military communications network linking huge and expensive mainframe computers is now accessible to anyone with a mobile phone. Americans today shop, bank, and work online. We play games, e-mail, keep up with the news, issue status updates, and spend countless hours exploring the Web. More than three quarters—81 percent —of all adults ages 18 and older go online, according to a December 2012 survey by the Pew Internet and American Life Project, a nonpartisan, nonprofit research center. Among teenagers and young adults, the share is even larger: 95 percent of teens ages 12-17 go online, as do 94 percent of young adults ages 18-29.

The Internet is celebrated as a haven of free speech and a beacon of free enterprise. But as its presence in our lives has grown, so have concerns about personal privacy and even national security. Ever-evolving technologies have led to new ways for corporations and the government to monitor our online movements without our knowledge. Advertisers are able to build detailed profiles of our behavior and interests by tracking which websites we visit. And whistleblowers like Edward Snowden and Julian Assange have used the Internet to raise serious questions about the ability of our government to keep us secure.

One of the biggest changes of the last decade has been the explosion of social networking sites, such as Facebook, Twitter, YouTube, Instagram, and Pinterest. Such sites allow people to post their own words, photos, and videos and to interact with hundreds, even millions, of "friends" or "followers." More than three-quarters (80 percent) of online teens and an equal share (83 percent) of young adults use social media sites. Online adults over 18 are the fastest growing segment of social media users: 67 percent of online adults used social networking sites in 2012, up from 46 percent in 2009. In October 2012, Facebook passed the one-billion-member mark.

But even as the "social Web" helps us express ourselves and create new communities, it blurs the distinction between public and private. We routinely disclose our opinions, upload our work history, broadcast our whereabouts, and share personal pictures and videos, sometimes without realizing that this information, once posted, can neither be reliably protected from widespread view nor permanently erased.

The same Internet that has given us new ways to socialize, learn, and engage in civic life has also given criminals new avenues to steal from us and scam us, often using information gleaned from public government documents now posted online. The same Internet that gives voice to the voiceless has allowed pornography, hate, and terrorist sites to flourish and made them more easily accessible. And because no one's in charge, there's no single authority we can call to complain.

When does our personal information become public? What data collection is acceptable? Should there be limits on what we can do online? It's time to find a way to balance our needs to safeguard privacy, preserve free speech, and ensure security for all our citizens, young and old.

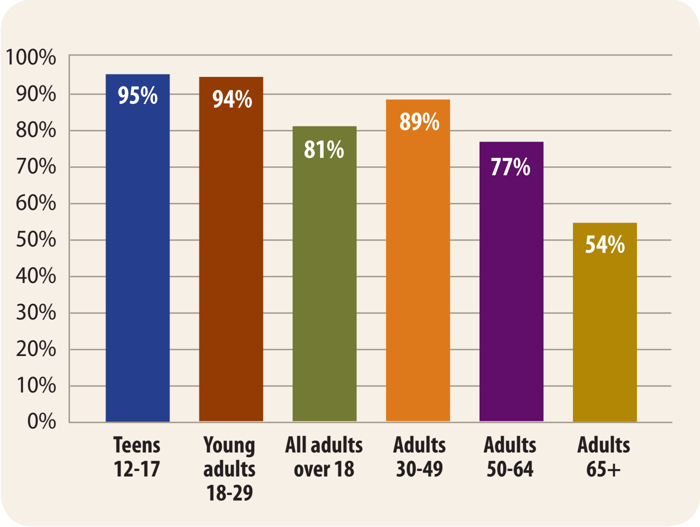
It's time to answer the question: *What should go on the Internet?*

This issue guide provides three different options for how to respond to that question. It avoids legal debates or discussion of the latest technological fixes; it aims instead to spur deliberations about sometimes conflicting things we hold valuable. Each option reflects a fundamentally different concern. Each concern suggests a course of action that we might take to address it, as well as the downsides or trade-offs of those actions.

- Option One: Protect individual privacy. Privacy, a fundamental American value, is now endangered by the Internet. Our top priority must be to safeguard personal information and safety on the Internet.
- Option Two: Promote freedom of speech and commerce. The Internet is a revolutionary leap forward for democratic societies and free markets. That freedom must be protected and encouraged.
- Option Three: Secure us from online threats. The Internet is a "Wild West" in which criminal activity can threaten our personal safety, national security, and economic vitality. Our top priority must be to curb such online activity and prevent it from harming law-abiding citizens.

By working through each option, we can come to our own individual and collective decisions about what we would support and under what conditions.

Who's Online?



Source: The Pew Research Center's Internet and American Life Project, December 2012

The National Issues Forums Institute
This issue guide was prepared for the National Issues Forums Institute in collaboration with the Kettering Foundation. Issue guides in this series are used by civic and educational organizations interested in addressing public issues. These organizations use the books in locally initiated forums convened each year in hundreds of communities. For a description of the National Issues Forums, log on to the website: **www.nifi.org**.

Other Topics and Ordering Information
Recent topics in this series include economic security, America's role in the world, immigration and higher education. For more information, please visit **www.nifi.org**.

Writer: Mary Engel
Executive Editor: Brad Rourke
Managing Editors: Tony Wharton and Ilse Tebbetts
Design and production: Long's Graphic Design, Inc.
Copy Editor: Lisa Boone-Berry

What Should Go on the Internet? Privacy, Freedom, and Security Online
Copyright 2013
National Issues Forums Institute
All rights reserved.
ISBN: 978-1-943028-17-7

Founded in 1927, the Kettering Foundation of Dayton, Ohio (with offices in Washington, DC, and New York City), is a nonprofit, nonpartisan research institute that studies the public's role in democracy. It provides issue guides and other research for the National Issues Forums. For information about the Kettering Foundation, please visit **www.kettering.org** or contact the foundation at 200 Commons Road, Dayton, Ohio 45459-2799.

Privacy is a fundamental American value. But the Internet has obliterated the line between public and private, forcing Americans to live in a virtual fishbowl. Our top priority must be to safeguard personal information on the Internet.

>>Protect Individual Privacy

LIKE MANY PEOPLE, Julia Angwin likes to window shop. Thanks to the Internet, she can do so from home. While browsing a store's website, she'll often move an expensive blouse or the perfect pair of shoes to her online shopping cart, even though she has no intention of buying them.

One day Angwin noticed something that doesn't happen when she window shops at the mall: a pair of shoes she'd coveted started following her. Almost every website she visited carried an ad featuring shoes she'd earlier put in her shopping cart.

Angwin is senior technology editor for the *Wall Street Journal*, so she knew about small files called cookies that websites install on our computers to "remember" our log-in names or what's in our shopping carts next time we visit. But it wasn't until she investigated targeted advertising for her newspaper that she learned the extent to which corporations are using these and more sophisticated tools to track and analyze our online movements.

Option One says that this is exactly the sort of thing we need to be on guard against as a society. Our lack of control over our personal information online leaves us vulnerable to scam artists, identity thieves, and stalkers.

Secrets for Sale

Angwin's *Wall Street Journal* investigation found that spying on Internet users is one of the fastest growing businesses on the Internet. Tracking companies assemble a profile of our interests as we visit different websites and then buy and sell our continually updated profiles on stock-market-like exchanges. It's not just when we are shopping online in front of our computers, either: Nordstrom's recently came under fire for tracking customers in its stores using their smartphones' WiFi capabilities.

Our taste in shoes, or which store departments we tend to frequent, are just some of the more benign secrets for sale. "Imagine that you've been searching for information about bipolar disease, and then every ad is targeting you as bipolar," Angwin said in an interview on National Public Radio's *Fresh Air*. "That seems creepy. That's when you get into the question of health data and financial data, or some of these things that . . . should be protected categories."

This option holds that privacy is a fundamental American value. Our right to live as we wish without overbearing scrutiny is as central to our democracy as the secret ballot. Corporations that track our online activities without our permission, or even knowledge, force Americans to live in a virtual fishbowl. Even worse, according to this option, are disclosures in 2013 about the US government's secret "PRISM" program, which evidently allows easy collection of private data from computers at Google, Yahoo, Skype, and others.

Voluntary Exposure

Invisible tracking is only one way the Internet has radically diminished our privacy.

Millions of people voluntarily post their job histories, virtual diaries, and videos of families and friends to social media sites, such as LinkedIn, Facebook, and YouTube, often without completely understanding just who has access to this information or how it might be used.

For example, more than three-quarters of US recruiters and human-resource professionals do online research when hiring for jobs, according to a Microsoft survey, and 70 percent report that they have rejected candidates because of information found on photo-sharing sites and discussion boards. Yet just 7 percent of job seekers surveyed believed that online information would affect their job search.

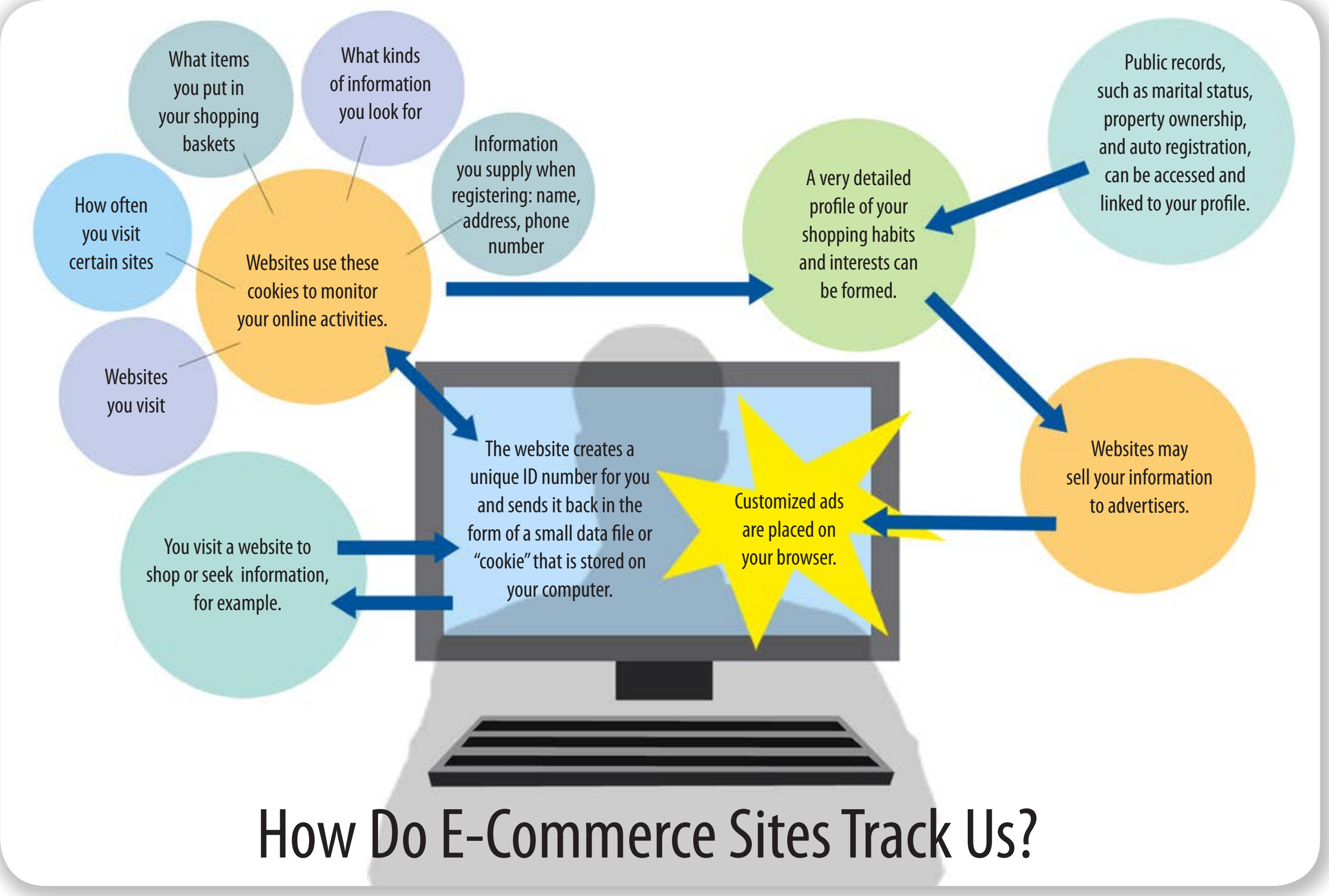
The rapid rise of cell phone and tablet "apps" has made it even easier for companies to glean such information. In 2012, the Federal Trade Commission (FTC) reached an agreement with Facebook that the social networking site would give members more tools to manage their privacy, and the agency fined Google $22.5 million for bypassing privacy settings to track users.

One simple way to protect our privacy, of course, is just not to post anything online. But these days, that means cutting ourselves off from many social and professional connections or coming across to prospective employers as technologically backward and, so, less desirable to hire.

There are other steps we can take. We can stop using "1234" or "password" as a password, update our personal settings to be more secure, and pay more attention to privacy policies.

But according to this option, being careful isn't enough. Think you can delete a Facebook page you thought was funny when you were a college freshman but now find just embarrassing? You'd likely be wrong. It is almost impossible to erase all record of it. And even if you're careful about your own Web use, friends and acquaintances who don't use privacy controls can post photos and embarrassing or inaccurate items about you.

Even information thought to be anonymous isn't always. Netflix, the movie-streaming service that allows viewers to rate movies online, released purportedly anonymous records of half a million customers as part of a now infamous contest to improve its rating system. Researchers were able to link the "anonymous" Netflix records to public data online and identify some users.


What items you put in your shopping baskets
What kinds of information you look for
Information you supply when registering: name, address, phone number
How often you visit certain sites
Websites use these cookies to monitor your online activities.
Websites you visit
Public records, such as marital status, property ownership, and auto registration, can be accessed and linked to your profile.
A very detailed profile of your shopping habits and interests can be formed.
The website creates a unique ID number for you and sends it back in the form of a small data file or "cookie" that is stored on your computer.
Customized ads are placed on your browser.
Websites may sell your information to advertisers.
You visit a website to shop or seek information, for example.

How Do E-Commerce Sites Track Us?

Public vs. "Peeping"

By law, some of the information about us is public. Births, marriages, and divorces are recorded in government documents. A driver's license is a public document, as are lawsuits and property records.

But, although always public, such records used to be harder to access. Individuals had to physically visit an office to inspect or copy a record, or at least send for it by mail. Now, they are increasingly made accessible online by the government.

This option points out that posting public records online makes it easier for people to obtain their own records—but also easier for direct marketers, employers, and private investigators to find them. Identity thieves who once had to dig through trash or steal mail to get Social Security numbers, credit card accounts, birth dates, and mother's maiden names can now mine such data online.

Information brokers who comb through public records and sell the information to online "people-finder" sites have made gathering such information easier still. The ease with which such information can be misused has prompted state-by-state policy debates about which records, if any, should be posted online.

What is worse, in the eyes of many, is the government's so-called PRISM eavesdropping system, the existence of which was revealed by whistleblower Edward Snowden. According to reports, PRISM allows law enforcement officials to eavesdrop on private e-mails, files, and communications from most of the major Internet companies in the United States. To get access, officials need to obtain approval from a secret court that only rarely, if ever, denies such requests.

Then there's the Google map service, Street View, which offers close-up photos of streets lined with homes and businesses. Option One holds that such detailed photos, while a boon for renters and homebuyers, are turning us into a nation of armchair "peeping Toms." "If the government were doing this, people would be outraged," Mary Kalin-Casey told the *New York Times* after Street View showed her cat, Monty, peering from her Oakland, California, apartment. Privacy concerns mounted even higher after Google acknowledged that the equipment in some of its street-view photography cars also collected private data from area WiFi networks. Google blamed the privacy breach on an engineering glitch; after an investigation, Germany ultimately fined Google $190,000 for the privacy violations.

Yet even Street View doesn't go as far as many cellphone apps, which actually can track your precise location without your knowledge.

Because the Internet is decentralized, no single authority exists to enforce privacy safeguards. The US Federal Trade Commission, the nation's consumer protection agency, has no authority unless online content is directed at children.

What We Could Do

This option holds that our top priority must be to safeguard personal information and safety on the Internet. To take full advantage of the Internet's rich resources, we need—and deserve—the same right to privacy online that we treasure offline.

Here are some things that this option suggests we could do, individually and collectively, along with some of the drawbacks:

- Businesses that collect data on people's Internet habits should display an easily understood and conspicuous privacy policy, allow people to control the dissemination of information they provide to a site, open up an individual's personal information file for his or her inspection, and protect the information collected. These are considered by the Federal Trade Commission to be standard "best practices" for collecting information, yet they report that just 20 percent of the busiest websites implement all four.

  But . . . *continually reading and signing consent forms would make using the Internet cumbersome and slow. Furthermore, limiting what companies can learn about their customers may discourage new commercial ventures and stifle innovation, limiting the Internet's potential to develop new products.*

- Governments should make court proceedings, marriage licenses, and other public records available the way they always have—on paper and in person. Posting them online makes it too easy for information brokers, con artists, identity thieves, and stalkers to get personal information from public documents.

  But . . . *to deny access to more efficient online records is to restrict our freedom to access public information. Online records make it easier for an adopted child to search for his or her birth parents, for individuals to research their genealogy, for a businesswoman to check out her prospective partner's background, for a reporter to investigate property scams, or for a detective to probe criminal activities.*

- Lawmakers should give the Federal Trade Commission wider authority to set privacy standards and publicly identify, fine, or shut down Web companies that violate them and misuse personal information.

  But . . . *overly rigid policing could discourage new commercial ventures. Allowing the FTC to audit Web companies raises the specter of government surveillance, giving a government agency access to personal information.*

These and other suggestions are shown in the table on p. 11.

OPTION TWO

The Internet is a revolutionary leap forward for democratic societies and free markets. Direct or indirect censorship by concerned citizens, special interests, or government could stifle this great resource.

>>Promote Freedom of Speech and Commerce

THE NONPROFIT, nonpartisan Sunlight Foundation uses the Internet to keep government honest. It puts government data online, then teaches citizen-researchers how to make sense of the information.

In early 2013, many citizens were using the data. Sunlight, Google, the MacArthur Foundation, and other partners, sponsored prizes for innovative citizen investigations. In one winning project, students at Stanford and Columbia universities used new disclosures of stock purchases by members of Congress to look for possible conflicts of interest.

That's just one example of how the Internet is transforming the practice of democracy. In the 2012 presidential campaign, voters did their own fact checking of political speeches, finding old video clips on YouTube that contradicted candidates' current positions. The nomination and election of Barack Obama is credited in large part to his ability to rally and organize supporters online.

Option Two holds that the rise of the Internet was the most revolutionary change for free societies and free markets of the 20th century. If its benefits are to persist into the 21st century, we will need to protect and nurture them.

A Fundamental Right

The Internet is an unprecedented tool for finding information and sharing it with the world. The case of Neda Agha Soltan showed what a powerful force it can be for promoting freedom. The young musician was shot during the protests following the 2009 Iranian election, and the powerful, shocking video of her death was broadcast online and viewed around the world.

"As millions watched an autocratic regime violently suppress dissent, we understood the Internet to be not just a source of information, fun and power, but a basic right—a right that is crucial to democracy, diplomacy and open government," wrote Julia Baird in *Newsweek*.

Two years later, the “Arab Spring” revolutions were spread, in large part, by online and mobile interactions as well as on Twitter and other social media sites.

Worldwide, four out of five people surveyed in 2012 by the Internet Society believed that access to the ideas and information available on the Internet should be a “basic human right.” Perhaps not surprisingly, the sentiment was more prevalent in China (92 percent), where sites like the Dalai Lama’s Web page and even movie databases are restricted, than in the United States (72 percent). Option Two holds that we should never take such Internet freedom for granted.

The Internet promotes equality, giving voice to the marginal, the different drummer, and the whistleblower. The former employee of an NSA contractor, Edward Snowden, revealed details of secret government surveillance programs to a news outlet with a primarily Internet-based readership, and continued to maintain a presence through online tools as he sought refugee status. One group that helped Snowden seek asylum was WikiLeaks, a website run by mostly nameless volunteers, which publishes leaked documents that governments, politicians, and corporations want kept secret. WikiLeaks has exposed a major bank’s tax evasions and climate scientists’ private e-mails. Its publication of classified reports from the Iraq and Afghanistan wars has been hailed as truth telling by some and treason by others.

Like democracy itself, the Internet can be raucous and messy. And, inevitably, some people want to tone it down or clean it up. According to this option, such efforts should be vigorously resisted. Direct or indirect censorship by concerned citizens, corporations, or government could stifle this great resource. Censorship, rules against anonymity, and efforts to turn the no-one’s-in-charge Internet into something akin to expensive and exclusive cable service are all attacks on Internet freedom.

Free Doesn’t Mean Easy

There’s no denying that the same Internet that spurs civil debate and democracy is also home to a proliferation of controversial, even hateful, sites. Neo-Nazis have websites, as do Holocaust deniers. Some sites promote beating up immigrants, or gays and lesbians. Others slur and degrade women. There are anti-Christian sites and anti-Islam sites. It’s enough to make a civilized person say, “There ought to be a law.”

But the fact is, there *are* laws—against child pornography and against the *practice* of violence and terrorism. Democracies rightly punish criminal actions. But not vile expressions. As a country that enshrines free speech, we have long believed that the best antidote to hate speech is speech that challenges, educates, and enlightens. As Supreme Court justice Louis Brandeis wrote in 1927: “If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence.”

Although not as ugly or frightening as hateful speech, incivility has long been a feature of the Internet—and also a challenge to defend. Outlawing anonymity is one proposed remedy that’s gaining momentum. Anonymous comments are a staple of websites and online bulletin boards, and the results are not always pretty. Such sites are roiling with statements that are mean, inflammatory, racist, and hateful. As the *American Journalism Review* notes, “The opportu-

The whistleblower
I can't allow the US government to destroy privacy and basic liberties
theguardian
guardian.co.uk

© Jerome Favre/epa/Corbis

Edward Snowden revealed details of secret government surveillance programs to news outlets and continued to maintain a presence through online tools as he sought refugee status.

nity to launch brutal assaults from the safety of a computer without attaching a name does wonders for the bravery levels of the angry."

According to Option Two, however, anonymous speech should be protected online, just as vigorously as it is protected offline. The United States, after all, was founded by pamphleteers writing anonymously. Alexander Hamilton, James Madison, and John Jay wrote the *Federalist Papers* under the pseudonym "Publius."

Protecting an Economic Engine

Everybody knows the hugely successful stories of Internet powerhouses, such as Facebook and Amazon. The Internet is an engine of innovation that fosters US competitiveness and productivity, contributing millions to the US economy.

A Harvard Business School marketing professor sought to quantify the economic impact of the Internet in a September 2012 report. He estimated that, directly or indirectly, the Internet employs 5.1 million people, or 2 percent of the US population, and produces $741 billion, or 5 percent of the country's gross national product (Google alone estimates its impact at $80 billion). But even beyond that, the Internet's social networking and information-gathering services fuel innovation and collaboration. And because many such online services are supported by advertising, they remain free and accessible to small businesses, scrappy startups, and the general public alike.

Overly burdensome regulations would stifle innovation, in this view. So would a less visible threat: lack of equal access to the networks that make the Internet possible.

Although the Internet may resemble a wide open Wild West, a relatively small number of major broadband carriers control the principal data routes that carry most of its traffic. If these companies start demanding extra money for transmitting videos and other materials requiring their highest speed connections, firms with deep pockets would enjoy speedy, first-class access while smaller players would be confined to slow-boat steerage. The head of Ticketmaster and Expedia, Barry Diller, told the *New York Times* that such charges would be "the equivalent of having the toaster pay for the ability to plug itself into the electrical grid."

This would throttle digital innovation and unfairly favor the big players, Option Two warns. This option favors so-called "net neutrality," in which everyone from small-shop gamers to Hollywood giants has equal access to the Internet.

The potential concentration of power in a few large companies has led public interest groups and many content creators to call for federal regulations to preserve today's relatively equal access for all players—a proposal that puts the community's devotion to free expression in conflict with its aversion to regulation.

What We Could Do

According to this option, the Internet is a revolutionary leap forward for democratic societies and free markets. Internet freedom must be protected and encouraged.

Here are some things we could do, along with the drawbacks of each action:

- Individuals and civil liberties groups should fight all efforts to censor the Web, ban controversial websites, or outlaw anonymity, and teach that the best antidote to controversial speech is more speech.

  But . . . *full freedom means anyone can post instructions for picking locks and building bombs. Hate groups and terrorists can recruit online. Sites such as WikiLeaks can put US troops and their allies at risk.*

- Schools and community groups should teach "information literacy" to students and other individuals, so people are better able to decide for themselves what is credible and what should be ignored.

  But . . . *this places much responsibility on individuals to protect themselves, essentially absolving wrongdoers. It also adds yet another subject that we hold schools responsible for teaching.*

- Congress should pass laws requiring that access to the Internet remain as open as possible for both entrepreneurs and consumers. We don't want to create a system of haves and have-nots by making individuals and companies pay for better access as they now do for cable television.

  But . . . *government regulation stifles innovation. Moreover, it could discourage Internet providers from investing in service improvements.*

These and other suggestions are shown in the table on p. 12.

The Internet is a Wild West of criminal activity that threatens our personal safety, our economic vitality, and our national security. Our top priority must be protecting our children and ourselves.

>>Secure Us from Online Threats

THE 2013 TRIAL and conviction of the latest so-called "Craigslist killer" provided a graphic look at the Internet's seamy side. Richard Beasley was sentenced to death for luring three men to rural Ohio with promises of agricultural employment . . . and then killing them.

A fourth man who escaped and later testified against Beasley said, "When he was shooting at me I saw nothing in his eyes." That case and several others turned a spotlight on the danger of cyberstalkers and serial killers using the Internet for their own ends.

This option holds that, while wrongdoers have lurked among classified personal ads for decades, the Internet has greatly magnified the problem and made it far too easy for the Richard Beasleys of the world. According to this option, we must guard against misuse of its freedoms.

The Dark Side

At its best, the Internet can be a community builder and matchmaker. E-mail and social networks allow us to keep in touch with distant family members and friends. We can share our passions for baseball or jazz with fans around the globe via websites and comment boards. A survey by Match.com, an online dating service, found that one in five singles has dated someone they've met online.

But the Internet has a dark side. Recipes for making methamphetamine, a major drug problem in rural America and one of the fastest growing drug threats in the nation, can be easily found online. Individuals' online financial, medical, and business transactions are vulnerable to hackers and thieves. Hate groups and terrorists use cyberspace to plan their activities and recruit new members.

Many of our concerns center on children. Few would argue that some websites can be harmful or disturbing to children, including sexually explicit or violent sites or ones that encourage unsafe behaviors, such as excessive drinking, abusing illegal drugs, or purging, an eating disorder all too common among teenage girls. Yet such material, which is widespread online, is constitutionally protected unless it contains child pornography, obscenity, or advocates violence against individuals.

As recently as the 1990s, protecting children online seemed as simple as keeping the family's Internet-connected computer in the kitchen or family room, where a parental presence would help ensure safe surfing. That's no longer true today, with Internet access available through cell phones, tablets, and other portable digital devices.

Hate Groups and Terrorists

Surveys show that parents' biggest online fear is of sexual predators. Often overlooked are the hate groups that are pervasive on the Web. Many such sites are specifically designed to appeal to children. The Los Angeles-based Simon Wiesenthal Center, a human rights group named after the Nazi-hunter Simon Wiesenthal, found in 2013 that while Facebook had made significant progress in curbing hate speech, its prevalence on Twitter had increased by 30 percent in the previous year. The report found more than 15,000 social networks, websites, forums, and blogs promoting violence, anti-Semitism, homophobia, hate, and terrorism.

Such groups can pose a threat to national security. Faisal Shahzad, who attempted to bomb Times Square; accused Fort Hood, Texas, army base shooter Maj. Nidal Hasan; and Boston Marathon bomber Tamerlan Tsarnaev; all legal US residents, are believed to have been inspired by the Internet postings of violent Islamic extremists.

In a *New York Times*/ CBS News survey commissioned shortly after the bombings, 66 percent of Americans said information about how to make bombs should not be allowed on the Internet.

Potentially even more dangerous are cyberattacks, in which hackers penetrate secure systems, even those of the Pentagon, for the purpose of stealing money and information or causing damage. Some of the recent cyberattacks are believed to have originated in China and Iran, and James Clapper, the US director of national intelligence, said in March 2013 that cyberattack had become the top security threat to the United States.

Under the banner of Internet freedom, law-abiding businesses and individuals can inadvertently aid criminals and terrorists by publishing information, including satellite- and street-level maps that make it easy for criminals to locate their victims. In this view, it is more important to protect people and nations than it is to protect the right to sell shoes and publish street maps.

"We can significantly advance security without having a deleterious impact on individual rights in most instances," Homeland Security Secretary Janet Napolitano told Fox News in June 2010. "At the same time, there are situations where trade-offs are inevitable."

What We Could Do

According to Option Three, the Internet's vaunted, no-one's-in-charge freedom has resulted in dangerous online activity that risks our personal safety, our economic vitality, and even our national security. This option holds that because the great power of the Internet can be harnessed for evil as well as for good, our top priority must be stopping such online activity, even if it means giving up some civil liberties to do so.

Here are some of the things that this option suggests we could do, along with some of the drawbacks:

- If online classified sites repeatedly carry prostitution ads, law enforcement should shut them down for enabling the illegal sex trade. Lawmakers should change laws that now protect such third parties.

  But . . . *shutting down such sites would put a damper on online entrepreneurship, a vital part of the US economy. Employees who had nothing to do with illicit ads would lose jobs. In addition, law enforcement would lose a way to track sex trafficking, since online activity leaves an electronic "footprint"—which, in the case of the Craigslist killers, enabled police to make an arrest.*

- Parents, schools, and libraries should use firewalls and other blocking technologies to keep young people from logging on to websites deemed inappropriate or from visiting social networks, such as Facebook or YouTube.

  But . . . *blocking young people's access to the Internet may also mean keeping a child from a troubled family from finding supportive networks or other helpful resources online. Libraries that use this technology would also block adults' access.*

- Because anonymity facilitates Internet crimes, the federal government should promote the creation of a public-private online identity-verification system. Under one government proposal, Internet users would voluntarily register with a secure "identity service provider" who confirms that they—and the registered users and services they interact with—are who they say they are. Consumers could choose from among a number of identity service providers.

  But . . . *even the most "secure" authentication records would be subject to subpoena, if not vulnerable to hackers. And due to liability concerns and other pressures, a voluntary verification system would effectively become mandatory. Whistleblowers and those with controversial or merely unpopular ideas would effectively be barred from using the Internet if they could not do so anonymously.*

These and other suggestions are shown in the table on p. 12.

SUMMARY

>>What Should Go on the Internet?

Privacy, Freedom, and Security Online

THE INTERNET IS an integral part of American life in the 21st century. Americans e-mail, instant message, blog, and tweet. We post photos, videos, and updates of our lives on Facebook and other social networking sites. We shop online, bank, work, play games, keep up with the news, and spend countless hours exploring the Web. Anything we need to know, we Google.

The decentralized, no-one's-in-charge Internet is celebrated as a place where freedom means innovation and all voices can be heard. But as its presence in our lives has grown—81 percent of US adults, and 95 percent of 12-to-29-year-olds now go online—so have concerns about personal and even national security.

Our every online move—and sometimes even our physical location—can be tracked, traded, and aggregated without our permission, or even knowledge. Children can all too easily find graphic pornography online, and anyone can find instructions for making methamphetamine or building bombs. Hate groups and terrorists actively use the Internet to plan and recruit.

When does our personal information become public? What data collection is acceptable? Should there be limits on what we can do online? The country needs to balance our needs to safeguard privacy, preserve free speech, and ensure security for all our citizens, young and old. This issue map summarizes three options about what should—and shouldn't—go on the Internet, suggesting what could be done and what could happen as a result.

OPTION ONE

Protect Our Privacy

Privacy is a fundamental American value. Our right to live as we wish without overbearing scrutiny is as central to our democracy as the secret ballot. But the Internet has obliterated the line between private and public, forcing Americans to live in a virtual fishbowl. Our lack of control over our personal information online can cost us jobs, ruin our reputations, and leave us vulnerable to scam artists, identity thieves, and stalkers, and even wrongful targeting by the government.

To take full advantage of the Internet's rich resources, we need—and deserve—the same right to privacy online that we treasure offline. Our top priority must be to safeguard personal information on the Internet.

***A primary drawback:** To have such privacy, we will have to put up with greater inconvenience and give up easy access to important information.*

EXAMPLES OF WHAT MIGHT BE DONE	SOME CONSEQUENCES AND TRADE-OFFS TO CONSIDER
Social networking sites should make privacy the default setting, requiring users to "opt in" to share information with various parties. Websites and search engines that collect data on users' Internet habits should obtain users' consent.	Rigid privacy settings may cause currently free social networking sites to start charging fees. Limiting what companies can learn about their customers could discourage new commercial ventures and stifle innovation online.
Information brokers—websites that provide personal information on individuals—should allow people to correct the information or block its distribution.	Individuals may have to give the brokers even more personal information to verify their identity, or pay a fee for anonymity, as is required to have an unlisted phone number.
Governments should make public records available the way they always have —on paper and in person. Posting them online makes it too easy for con artists, identity thieves, and stalkers to get personal information from public documents.	Denying access to online records restricts our freedom to access public information. Online records make it easier for adopted children to search for their birth parents, people to explore their genealogy, a reporter to investigate property scams, or a detective to probe criminal activities.
The best way to protect personal information is to keep as much of it as possible off the Internet. Don't bank or shop online. Don't post profiles, résumés, photos, or other identifying materials.	Jobs and promotions would suffer because employers expect workers to be sufficiently Internet-savvy to have online profiles. Consumers would miss out on better interest rates and other deals offered by online banks and businesses.
Congress can require that the workings of the secret courts overseeing the intelligence gathering involving the online accounts of American citizens, such as the PRISM program, be subject to greater control and play a stronger watchdog role.	This may endanger national security, as such electronic "eavesdropping" has been credited with stopping more than one terrorist attack.

OPTION TWO

Promote Freedom of Speech and Commerce

The Internet is a revolutionary leap forward for democratic societies and free markets. It promotes equality, giving voice to the marginal, the whistleblower, the different drummer. It's an unprecedented tool for finding information and sharing ideas. It's an economic engine that fosters innovation and drives US competitiveness and productivity.

But direct or indirect censorship by concerned citizens, special interests, or government, attacks on anonymity, and efforts to turn the no-one's-in-charge Internet into something akin to expensive and exclusive cable service are all attacks on Internet freedom and should be vigorously resisted.

***A primary drawback:** Greater freedom on the Internet may make it easier for hate speech and criminal activity to flourish.*

EXAMPLES OF WHAT MIGHT BE DONE	SOME CONSEQUENCES AND TRADE-OFFS TO CONSIDER
Rather than blocking Internet access, schools can teach K-12 children how to use the Internet safely.	Schools would control access and teach values, which are responsibilities that rightly belong to parents.
Internet users should rigorously oppose efforts to ban anonymous comments on websites. Anonymity is a cornerstone of free speech and a deeply entrenched American tradition.	Under cover of anonymity people post crude, cruel, and racist comments that they would never own up to if they had to identify themselves. Anonymity allows con artists, thieves, and terrorists to thrive online.
The best antidote to controversial speech is more speech. Individuals and civil liberties groups should fight all efforts to censor the Web or ban websites.	Full freedom means anyone can post instructions for making methamphetamine and building bombs. Hate groups and terrorists can recruit online.
Schools and community groups should teach "information literacy" so people are better able to decide for themselves what is credible and what should be ignored.	This puts too much responsibility on users to protect themselves, while absolving wrong-doers. It also adds another subject we would make schools responsible for teaching.
Congress should pass laws requiring that access to the Internet remain as open as possible for everyone. We don't want to create a system in which some people can afford to pay for better access than others.	More government regulation could discourage Internet providers from investing in service improvements.

OPTION THREE

Secure Us from Online Threats

The Internet is a Wild West of criminal activity that threatens our personal safety, our economic vitality, and our national security. Social networks are pick-up sites for child predators. Online classifieds serve as red-light districts for prostitutes. An economy increasingly dependent on online transactions is vulnerable to hackers and thieves, and our nation's critical infrastructure is wide open to cyberterrorists.

Because the great power of the Internet can be harnessed for evil as well as for good, our top priority must be stopping such online activity, even if it means giving up some civil liberties to do so.

***A primary drawback:** To have such security, we will necessarily have to give up a certain amount of freedom and even privacy.*

EXAMPLES OF WHAT MIGHT BE DONE	SOME CONSEQUENCES AND TRADE-OFFS TO CONSIDER
If online classified sites repeatedly carry prostitution ads, law enforcement should shut them down for enabling the illegal sex trade. Lawmakers should change laws that now protect such third parties.	Employees who had nothing to do with illicit ads would lose jobs. And users would lose a convenient and affordable way to sell a couch and find an apartment.
Parents, schools, and public institutions should use technology to block offensive sites. Schools should also ban cell phones and block social networking sites where anyone can "friend" a child.	Blocking access means missed opportunities to teach Internet safety and critical thinking. Libraries using blocking technology intended for children can end up blocking access by adults.
Sites that publish national security leaks or show videos that could endanger troops or public safety should be shut down and their operators prosecuted for espionage.	Assuming that the site operators were not involved in stealing the information, prosecuting them for publishing it would violate their free speech rights.
Because anonymity facilitates Internet crimes, the federal government should promote the creation of a public-private online identity-verification system.	Online identity verification is an assault on privacy. Whistleblowers and those with unpopular ideas would effectively be barred from using the Internet if they could not do so anonymously.
Congress should support and even beef up laws that give the FBI expanded powers to seize electronic records and monitor e-mail.	Such expansive laws are a grave invasion of privacy for all Americans and risk turning the United States into a police state.