How do we realistically assess the past, present, and future of our security and privacy technology? Like Spider-Man, with our great computing power comes great responsibility—to use our power wisely, to design high-quality security and privacy applications, and to quickly correct errors and improve results. The difficulty of predicting the future of security and privacy is often accompanied by arrogance about our abilities to understand issues and solve problems effectively. But this scientific hubris can also be an opportunity to look back, applaud our successes, evaluate our mistakes, and take corrective action.

This article is my last as editor in chief of IEEE Security & Privacy. It’s also my last professional article; I’m refocusing my efforts on helping mend America’s fraying social safety net. So it seems appropriate to look closely at security and privacy in a societal context: how we got here, where we are now, and what we need to ensure that we use our great power responsibly.

How We Got Here
In 1951, Lord Bowden reported this conversation with Professor Douglas Hartree, the builder of England’s first differential analyzer:1

He told me that, in his opinion, all the calculations that would ever be needed in this country could be done on the three digital computers which were then being built—one in Cambridge, one in Teddington [at the National Physical Laboratory] and one in Manchester. No one else, he said, would ever need machines of their own, or would be able to afford to buy them. He added that machines were exceedingly difficult to use, and could not be trusted to anyone who was not a professional mathematician, and he advised [UK electronics firm] Ferranti to get out of the business and abandon the idea of selling any more.

I. Bernard Cohen assures us that Howard Aiken, a designer of IBM’s Mark I computer, made a similar statement in 1952:2 “Originally one thought that if there were a half dozen large computers in [the US], hidden away in research laboratories, this would take care of all requirements we had throughout the country.” Clearly, we computer scientists (like many other professionals) are not very good at peering into the future. In fact, Lord Bowden was quite blunt: “It is amazing how completely wrong a great man can be.”

“The Rugged Manifesto,” described in the sidebar, points out that “code will be used in ways I [the developer] cannot anticipate, in ways it was not designed, and for longer than it was ever intended.” This statement encapsulates how we got from a small network designed for collaboration to a global technology infrastructure on which much of the world’s functioning depends. Let’s look more carefully at this evolution, because its course hints at what we can do to harness and apply our power.

Many of you know the history of the Internet and its genesis from small US defense project to mammoth, interconnected infrastructure. Just as Hartree and Aiken thought too small, so did the Internet’s builders. When the first “worm” infected the Internet in 1988, many people were surprised; they saw the Internet as a mechanism for education and collaboration, not a vector for mischief or malice. As Virginia Tech historian Janet Abbate notes, “They thought they were building a classroom, and it turned into a bank.”

What were technologists and policymakers thinking during the US government’s initial foray into building an electronic infrastructure? Kirk Lougheed, one of the inventors of the Border Gateway Protocol (BGP), notes that, “In the early days of the Internet, getting stuff to work was the primary goal. There was no concept that people would use this to do malicious things. … Security was
not a big issue.” That function-first mentality continues today: functionality über alles, implemented quickly. "Nash," a member of L0pht, an early hacker collective, describes this philosophy: "It’s get it up, get it running as fast as we can. Let’s make some money. ... There’s this tremendous push to get code out the door, and we’ll fix it later."4

But David Clark, MIT computer scientist, dispels the notion that Internet designers never thought about security. He says, "It’s not that we didn’t think about security. ... We knew that there were untrustworthy people out there, and we thought we could exclude them."3

The next step toward insecurity occurred when packet-switched communications replaced telephone networks: technologists traded a stable design for one that was inherently riskier. To see why, examine where intelligence resides in each type of network. The public switched-telephone networks’ design reflected the phone companies’ investment in their own capabilities—a system that is smart in the center and dumb at the edges. That is, the phone companies’ switches ran everything, with little intelligence in business or personal handsets. The Internet’s design is the reverse: the network simply carries data, but the edges are smart. "The center is a computationally powerful but fundamentally dumb collection of routers and transmission channels."5 The central design makes it easy for new users to join the network.

But this lack of smarts has a security price: it’s difficult to provide centralized security and privacy. In the Internet’s early days, when the users knew and trusted one another, this price didn’t much matter. As more people joined the network, the equation changed. The resulting design is more like the Wild West, perhaps because of an underlying principle of caveat emptor—let the buyer beware. “From its unlikely roots in a Pentagon research agency, the Internet developed into a global communications network with no checkpoints, no tariffs, no police, no army, no regulators and no passports or any other reliable way to check a fellow user’s identity. Governments would eventually insinuate themselves into cyberspace—to enforce their laws, impose security measures and attack one another—but belatedly and incompletely."3

In other words, the Internet architecture leaves Internet users to protect themselves; few inherent design constructs assure security and privacy in Internet traversals and transactions. The trust model relies largely on the parties involved to be who they say they are, affiliated with the organizations they say they are with, taking the actions they say they are taking, and leading to the results they claim to be realizing. Clearly, this model has huge weaknesses; among other sites, the Risks Forum (http://catless.ncl.ac.uk/Risks) illustrates that the Internet is rife with weaknesses that have long been accidentally and intentionally exploited.

With Greater Power Comes Greater Responsibility

But that was then and this is now. In the interim, several players have tried to be more responsible, by warning others, protecting their own sites and users, or providing services and applications that offer protection.

For example, as early as 1973, Ethernet coinventor and 3Com founder Bob Metcalfe warned about significant risks, telling the Arpa Network Working Group that it was very easy for outsiders to log in to the network. He wrote, “All of this would be quite humorous and cause for raucous eye winking and elbow nudging, if it weren’t for the fact that in recent weeks at least two major serving hosts were crashed under suspicious circumstances by people who knew what they were risking; on yet a third system, the system wheel password was compromised—by two high school students in Los Angeles no less. We suspect that the number of dangerous security violations is larger than any of us know [and] is growing.”6

Even when we know about risks, we often ignore them. For instance, the 1988 Morris Worm exploited buffer overflows, a problem identified two decades earlier. Today’s news media continue to report buffer overflow–based attacks and accidents.

Similarly, the BGP (sometimes called the Napkin Protocol because several computer scientists devised it on table napkins while brainstorming the solution to a routing problem) was full of security holes. "Warnings about the risks inherent in BGP are almost as old as the protocol itself. ‘I knew that routing security was a problem,’ Columbia University computer scientist Steven M. Bellovin said. ‘Seeing this conceptually is fairly easy and straightforward. Sorting it out in terms of the engineering is fiendishly difficult.’"7

Boston University professor Sharon Goldberg recently asked why BGPSEC, a solution to the two-decade-old problem, still isn’t deployed.8 The answer rests with the Internet’s size and complexity and the need for substantial numbers of users to change their ways. "BGP is a global protocol, running across organizational and national borders. As such, it lacks a single centralized authority that can mandate the deployment of a security solution; instead, every organization can autonomously decide which routing security solutions it will deploy in its own network. Thus, the deployment becomes a coordination game among thousands of independently operated networks. This is further complicated by the

---

IEEE Security & Privacy  
November/December 2015
fact that many security solutions do not work well unless a large number of networks deploy them.

In fact, Internet-related actors often work toward different ends. The common purpose that launched and nurtured it no longer prevails. There are, and have been for some time, important and powerful players that make up the Internet milieu with interests directly at odds with each other. The Internet is not a single happy family of people dedicated to universal packet carriage. There is contention among the players. ... The technical architecture must accommodate the tussles of society while continuing to achieve its traditional goals of scalability, reliability, and evolvability. This expansion of the Internet’s architectural goals is a difficult, but central technical problem.

Indeed, vendors sometimes try to build security and privacy in, just as security experts suggest. But even then, users push back, based on arguments about cost, complexity, or convenience. For instance, Guardian technology reporter Alex Hern analyzed the privacy implications of Microsoft’s recently issued Windows 10 operating system. He notes that, “The European digital rights organisation (EDRi) sums up the company’s 45 pages of terms and conditions by saying: ‘Microsoft basically grants itself very broad rights to collect everything you do, say and write with and on your devices in order to sell more targeted advertising or to sell your data to third parties’.”

But some argue that Microsoft is acting responsibly, giving users flexibility in some cases and forcing good security and privacy practice in others. “Users have attacked Windows 10 for only offering two settings when it comes to Windows Update: either install and restart immediately, or install and ask permission to restart. The option to not install updates does not appear to be present on the base version of the OS. But that decision chimes with the advice of security experts, who say that the number one thing for staying safe online is to install every security update immediately.”

In many cases, a security practice is effective only when everyone implements it; BGPSEC is an example of how a few holdouts can intervene to impose structure, guidance, standards, or penalties on security practice. But well-intentioned interventions that sound perfect in theory don’t always work well in practice. For instance, consider the effects of Europe’s imposition of a right to be forgotten. This right is often expressed as an argument about fairness: in erasing erroneous online material or evidence of our youthful mistakes, we eliminate material that could unfairly keep us from future opportunities. But Harvard’s Jonathan Zittrain points out that “the practice of shaping what stays and what goes from the database is hopelessly individualistic. By allowing the delisting of information that is incorrect, outdated or harmful for individuals, who knows what else will follow. It sets us on a path … where the internet becomes the lowest common denominator result of what all the world’s countries and courts are prepared to leave behind.”

There are many other examples of inherent unfairness in the way the Internet works. For instance, Latanya Sweeney, chief technology officer of the US Federal Trade Commission, demonstrated that the targeted advertisements Google’s search engine shows its users differ dramatically based on perceived racial differences derived from a user’s name. It’s not clear whether the bias comes from the way the search engine provides advertising or whether Google is merely reflecting society’s bias. What is clear is that the bias is strongly reflected in advertisement choices.

What about using our technology to create algorithms that implement fairness and balance? Perhaps we can design programs that are race neutral, gender neutral, or otherwise unbiased. Then voluntary agreements or even regulation

**Internet architecture leaves Internet users to protect themselves; few inherent design constructs assure security and privacy in Internet traversals and transactions.**
could impose fairness rules, as happens in advertising or banking. 13 Unfortunately, this is easier said than done. In an interview, Microsoft Research’s Cynthia Dwork identifies significant biases in the algorithms we use to make decisions and predictions. Indeed, algorithms attempting to be fair can sometimes bias decisions even more. “Design choices in algorithms embody value judgments and therefore bias the way systems operate. … These things are subtle: For example, designing an algorithm for targeted advertising that is gender-neutral is more complicated than simply ensuring that gender is ignored. … [Classification rules obtained by machine learning are not immune from bias, especially when historical data incorporates bias.” 14

Similarly, facial recognition software relies on algorithms for identification and authentication: good security and privacy goals but with a flawed implementation. Use of facial recognition software is increasing, even though its error rate can be as high as 20 percent. It is “being eagerly adopted by dozens of police departments around the country to pursue drug dealers, prostitutes and other conventional criminal suspects. But because it is being used with few guidelines and with little oversight or public disclosure, it is raising questions of privacy and concerns about potential misuse.” 15

A Needed Course Correction
Today, information technology is embraced by or embedded in almost everything, from applications remotely controlling your home devices to collision-avoidance software for automobiles. Much of it holds great promise to save energy, money, and lives. But the public trusts technology more than is deserved. Technology is often fielded when it’s good enough, even if it hasn’t been fully tested. “It’s closer to an assemblage of kludges … surviving only because of an industry-wide penchant for patching over problems rather than replacing the rot.” 16 When we add the Internet to the mix, vulnerabilities in Internet design and implementation become pathways that enable malicious actions. Exacerbating these problems is the nature of the supply chain: we build systems (hardware and software) from parts we purchase or commission from other suppliers. This decentralization makes it difficult for manufacturers to ensure that individual parts have the latest updates and that these updates work well together. Feature interaction—the unanticipated interference of one function by another—has been a known, unsolved problem in the telecommunications industry for decades, 17 and complex supply chains amplify its adverse effects.

Abandoning the Internet is certainly not an option, and embracing new business models is difficult and can take decades. After all, most technologies have had long adoption periods with gentle slopes, even in the US. Nevertheless, we need a course correction soon, because the clamor for change is growing—especially as cyber is considered to be an option in warfare 18 and businesses rush to move their products to the Internet of Things. Indeed, many of the individuals and enterprises building and selling these connected products fail to consider the risks of embedding software in items and then connecting them in networks. “The selling point for these well-connected objects is added convenience and better safety. In reality, it is a fast-motion train wreck in privacy and security.” 19

The press, in its zeal to notify the public, often oversstates the scale of Internet-related risks. But the press is stepping in where businesses are reluctant to highlight problems. As a result, the growing number and kinds of problems, many of which are difficult or impossible to resolve after they occur, are increasingly on the public’s radar. Major newspapers such as the New York Times and the Guardian frequently write editorials about Internet issues, and even law textbooks note that it’s increasingly easy for criminals to perpetrate crimes and hide on the Internet. 19

Business shares the blame, but so do we, as security and privacy practitioners, researchers, and policymakers. “In designing the network, [Internet Hall of Famer Steve] Crocker said, ‘We could have done more, and most of what we did was in response to issues as opposed to in anticipation of issues.” 20

Step by Step
Crocker’s comment is, in some sense, the basis for our next steps. We need to review how we might have anticipated issues, rather than waiting for problems and then patching them.

What concrete steps can we take right now to put us on the path to a more secure and privacy-protected technology infrastructure? To begin, we can encourage business to abandon the Wild West mentality, with “its purely libertarian ethos and Pollyannaishness about technology.” 20 I propose we do this through better education, context, and coordination.

Better Education
The need for cybersecurity professionals has been described as great and immediate. So, in many countries, government and business are pushing people into cybersecurity careers. Courses and programs abound to teach the uninitiated a handful of security techniques. For example, a Symantec security specialist posted his list of requirements for entering a security career: understanding TCP/IP and a bit about an operating system, learning
about intrusion detection systems, setting up firewalls and routers, being able to read code, ‘and if necessary modifi[ing] or debug[ging] programs and scripts, ... knowing how to debug code ... {and familiarizing} yourself with the concept of penetration testing.’

Short courses are especially appealing; in fact, almost anyone can complete a three-month course and become a developer, without any dependability, security, or privacy training.

We need saner policies about who designs and builds our information infrastructure: whom to educate, how, and for how long. It’s unacceptable to give “security expert” status to anyone who can breathe and run a virus checker. As with any other essential profession, we must differentiate novices from masters and experts and recognize that expertise and experience in one security aspect doesn’t enable someone with narrow programming skills to perform solid security analysis and design or effective penetration testing. Although many organizations and governments are creating certificate and advanced degree curricula, the need is outstripping supply. It’s time to stop putting unskilled and inexperienced workers into cybersecurity positions.

**Better Context**

Our technology is not conceived, created, or used in isolation. Rather, it’s always embedded in a social context that interacts with the technology and its users. "Technology in isolation, not embedded in any network of human and nonhuman actors, has nothing to stabilize. It is the whole actor network (as distinct from the Internet as a network of technology) that becomes stable, as all the human and nonhuman actors align and harmonize themselves to common (socio-technical) interfaces." So we must consider current and proposed innovations in context. At the extreme, we don’t want to overreact and dismiss promising or proven technologies because of single categories of use. For example, several high-visibility technologists have warned of artificial intelligence’s (AI’s) dangers. "In October [2014], Elon Musk called AI ‘our greatest existential threat,’ and equated making machines that think with ‘summoning the demon.’ In December, Stephen Hawking said ‘full [AI] could spell the end of the human race.’ And this year, Bill Gates said he was ‘concerned about superintelligence,’ which he appeared to think was just a few decades away. But the real worry, specialists in the field say, is a computer program rapidly overdoing a single task, with no context. A machine that makes paper clips proceeds unfettered, one example goes, and becomes so proficient that overnight we are drowning in paper clips.’

A more focused example, set in context, is an open letter that a large number of technologists signed and presented at the 2015 International Joint Conferences on Artificial Intelligence. It suggests banning the use of [AI] to make autonomous weapons. Evaluating this proposal in this context is far more reasonable than banning AI outright.

And the context should involve aspects of the society in which the technology will be used. Take University of Texas professor Michael Webber’s analysis of America’s surging interest in renewable energy. Only 40 years ago, the US worried about its dependence on oil; now it’s in the midst of creating a robust, diverse energy infrastructure that many said couldn’t be done. Why? The convergence of three things: "highly functioning markets; stable, forward-thinking policies; and disruptive technologies. ... [M]arkets, policies, and technologies are all pointing in the same direction—which is up—and the result is powerful. It goes to show that a public–private–technological partnership is transformative.”

We can use the same triumvirate to provide context, support analysis, and implement more responsible technology.

**Better Coordination**

However, these triumvirate members haven’t traditionally worked well together. To provide sensible context, these and other parts of society must better coordinate. For example, several highly visible automobile hacking incidents were recently reported in the press. In such cases, when a vulnerability is discovered, should researchers report it to business or government before publishing their research papers? Once notified, should business and government notify consumers? There have been many shameful cover-ups to save face or sales or both, sometimes significantly harming technology users. A coordinated, contextual solution involves all parties with a stake in the outcome. "Both researchers and companies are going to need to meet somewhere in the middle ... if the goal is to make products safer for consumers as soon as possible. Perhaps the most important step a company can take is coming up with a coordinated disclosure policy, a set of public guidelines for how it will respond when researchers come forward with problems.’

One of the first questions should be asked at the design stage: Does this product or service need this technology? It’s in the midst of creating a robust, diverse energy infrastructure that people develop and use.
A Rugged Manifesto

In September 2012, “The Rugged Manifesto” appeared online (www.ruggedsoftware.org), challenging developers to acknowledge their software’s shortcomings:

I am rugged and, more importantly, my code is rugged.
I recognize that software has become a foundation of our modern world.
I recognize the awesome responsibility that comes with this foundational role.
I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.
I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic and national security.
I recognize these things—and I choose to be rugged.
I am rugged because I refuse to be a source of vulnerability or weakness.
I am rugged because I assure my code will support its mission.
I am rugged because my code can face these challenges and persist in spite of them.
I am rugged, not because it is easy, but because it is necessary and I am up for the challenge.

But being “rugged” and writing “rugged code” are easier said than done.

this technology? Years ago, one of my clients added software to its devices, even though the analog versions of its products were more reliable than the digital ones. The reason? The company thought it needed software to compete in the market. A 2015 Guardian editorial elaborates on similar decisions by automobile manufacturers.26

You may ask why a car needs an internet address in the first place. The bad answer is that lots of other cars have them now, so any new model will want one. The good answer is that computer networks are transforming the world, and in many ways to our benefit. Networks, by their nature, have a tendency to grow—and to grow more valuable as they do. But they have to be secure; and since it is impossible to make them entirely secure, they must also be designed to fail gracefully and as safely as possible. This requires changes in engineering culture, but also in the wider corporate culture: companies that make things need to learn the hard lessons about openness that have been forced onto software companies in the past 20 years. It took the mainstream software industry years to understand that rewarding reports of security holes with bounties, rather than letting them be sold on the dark market, is sensible and necessary. We do not have that time now that software is so ubiquitous that it is invisible. We are moving towards a world where almost everything will have a computer inside it, and those computers will want to talk to the outside world, either to receive instructions or to report on what is happening around them. This is what is meant by the internet of things. How can we stop it becoming an internet of things that can kill us, or spy on us?

The answer to successful security and privacy implementation must be multidisciplinary and contextual. Its elements involve an understanding of ethics and behavioral science. We can evaluate a technology’s potential effects—both costs and benefits—by simulating likely usage and outcomes. And we can probe its unanticipated (and possibly adverse) effects by using sophisticated testing and adversarial thinking. This approach is much harder than writing code—it requires a team of experts who know a lot more than how to use the latest intrusion detection system. In particular, the team must constantly imagine what could go wrong and what the consequences might be.

Because we’re human, we can’t expect market forces and good wishes alone to lead to better software, systems, and societies. Regulation and oversight play a role, and many in the press, including the New York Times editorial board, are calling for regulation of automobile, medical device, and other software types.27 If well coordinated, this triumvirate of technology, markets, and policies should push us to implement and sustain better security and privacy. “Companies and governments, too, must realise that if a world of interconnected, highly capable and almost intelligent widgets is to be safe, they must be constantly expecting that it will be unsafe, and actively collecting knowledge about the ways in which it can—and will—be dangerous.”27

We are developing technology that’s increasingly powerful, not only in manipulating hardware and data but also in creating opportunities and changing peoples’ lives. Building and sustaining more pervasive and powerful technology require us to take more responsibility for our ideas and actions. So pin a Spider-Man picture to your office wall to remind you of that responsibility.

We aren’t the first discipline to learn to view our technology as only one aspect of a large, evolving world
that’s built by and functioning within its societal context. Author Joseph Conrad spent significant time on sailing vessels, in part to inform his writing. "He recognized that technological progress, for all its much-heralded benefits, comes with social and ethical costs. To operate a sailing ship was to master a 'craft.' You had to observe and interpret nature, adapt and react to fast-changing conditions, obey without question, decide without doubt, toil without pause. The craft connotes more than a clutch of skills; it is a code for how to live. It turns a sailing ship into a 'fellowship,' a community forged by shared values."28 We too must think of ourselves as active members working in a diverse society. We are more than a clutch of skills—we can use our technological insights and abilities to understand differences, articulate common goals, and enable the community forged by shared values.

References
Erratum

In Robin Bloomfield’s From the Editors article in the September/October issue, pp. 3–4, the sentence should read, “This, as well as the updates to the UK strategy that are being discussed now and will lead to a refresh in 2016...”