PewResearchCenter

NUMBERS, FACTS AND TRENDS SHAPING THE WORLD

FOR RELEASE DECEMBER 18, 2014

Digital Life in 2025

The Future of Privacy

Experts believe the struggle over privacy and tracking policies will extend through the next decade. They are divided about the likely future. Some expect that governments and corporations will continue to expand upon the already prevalent tracking of people's personal lives and the data-basing and monetization of personal information. Others expect it may be possible that new approaches will emerge to enable individuals to better control their identities and exercise more choice about who knows what.

FOR FURTHER INFORMATION ON THIS REPORT:

Lee Rainie, Director, Internet, Science, and Technology Research, Pew Research

Janna Anderson, Director, Elon University's Imagining the Internet Center

202.419.4372

www.pewresearch.org

RECOMMENDED CITATION: Pew Research Center, December 2014, "The Future of Privacy"
Available at: http://www.pewInternet.org/2014/12/18/future-of-privacy/

About This Report

This report is the latest in a sustained effort throughout 2014 by the Pew Research Center's Internet Project to mark the 25th anniversary of the creation of the World Wide Web by Sir Tim Berners-Lee (The Web at 25). It includes the responses of hundreds of experts to a question about the future of privacy in the coming decade. It is part of a series of reports tied to the Web's birthday; some of the studies look at how far Internet use has penetrated people's lives and some examine experts' assessments of the technology environment by 2025. The findings we describe in this report emerge in the context of these earlier reports:

- A February 2014 report from the Pew Research Center's Internet Project tied to the Web's anniversary looking at the strikingly fast adoption of the Internet and the generally positive attitudes users have about its role in their social environment.

- A March 2014 *Digital Life in 2025* report issued by the Pew Research Center in association with Elon University's Imagining the Internet Center focusing on the Internet's future more broadly. Some 1,867 experts and stakeholders responded to an open-ended question about the future of the Internet by 2025.

- A May 2014 *Digital Life in 2025* report on the Internet of Things from Pew Research and Elon University examining the likely impacts of the Internet of Things and wearable and embedded networked devices. A majority of the more than 1,600 respondents said they expect significant expansion of the Internet of Things, including connected devices, appliances, vehicles, wearables, and sensor-laden aspects of the environment.

- A July 2014 *Digital Life* report on "Net Threats" (challenges to the open Internet) from Pew Research and Elon University canvassing a number of experts and other stakeholders on what they see as the major threats to the free flow of information online. A majority of these experts expect the Internet to remain quite open to sharing but they see many potential threats to this freedom.

- An August 2014 *Digital Life* report on "AI, Robotics, and the Future of Jobs" from Pew Research and Elon University about the degree to which technology advances might destroy more jobs than they created. The expert respondents were split on the verdict.

- An October 2014 *Digital Life* report on "Killer Apps in the Gigabit Age" from Pew Research and Elon University about the potential new digital activities and services that will arise as gigabit connectivity—50 to 100 times faster than most Americans now enjoy—comes into communities.

- A later October 2014 *Digital Life* report on "Cyber Attacks Likely to Increase" from Pew Research and Elon University looked at experts views about the prospects for attacks on nation-states, key utilities and other industries, and on consumers.

This report is a collaborative effort based on the input and analysis of the following individuals:

Lee Rainie, *Director, Internet, Science and Technology Research*
Prof. Janna Anderson, *Director, Elon University's Imagining the Internet Center*

Find related reports about the future of the Internet at
http://www.pewInternet.org/topics/future-of-the-Internet/

About Pew Research Center

Pew Research Center is a nonpartisan fact tank that informs the public about the issues, attitudes and trends shaping America and the world. It does not take policy positions. It conducts public opinion polling, demographic research, media content analysis and other empirical social science research. The center studies US politics and policy views; media and journalism; Internet and technology; religion and public life; Hispanic trends; global attitudes; and US social and demographic trends. All of the center's reports are available at www.pewresearch.org. Pew Research Center is a subsidiary of The Pew Charitable Trusts.

About the Imagining the Internet Center at Elon University

The Imagining the Internet Center's mission is to explore and provide insights into emerging network innovations, global development, dynamics, diffusion and governance. Its research holds a mirror to humanity's use of communications technologies, informs policy development, exposes potential futures, and provides a historic record. It works to illuminate issues in order to serve the greater good, making its work public, free and open. The center is a network of Elon University faculty, students, staff, alumni, advisers, and friends working to identify, explore, and engage with the challenges and opportunities of evolving communications forms and issues. They investigate the tangible and potential pros and cons of new-media channels through active research. The Imagining the Internet Center sponsors work that brings people together to share their visions for the future of communications and the future of the world.

Table of Contents

Summary

The terms of citizenship and social life are rapidly changing in the digital age. No issue highlights this any better than privacy, always a fluid and context-situated concept and more so now as the boundary between being private and being public is shifting. “We have seen the emergence of publicy as the default modality, with privacy declining,” wrote **Stowe Boyd**, the lead researcher for GigaOm Research in his response in this study. “In order to ‘exist’ online, you have to publish things to be shared, and that has to be done in open, public spaces.” If not, people have a lesser chance to enrich friendships, find or grow communities, learn new things, and act as economic agents online.

Moreover, personal data are the raw material of the knowledge economy. As **Leah Lievrouw**, a professor of information studies at the University of California-Los Angeles, noted in her response, “The capture of such data lies at the heart of the business models of the most successful technology firms (and increasingly, in traditional industries like retail, health care, entertainment and media, finance, and insurance) and government assumptions about citizens' relationship to the state.”

This report is a look into the future of privacy in light of the technological change, ever-growing monetization of digital encounters, and shifting relationship of citizens and their governments that is likely to extend through the next decade. “We are at a crossroads,” noted **Vytautas Butrimas**, the chief adviser to a major government's ministry. He added a quip from a colleague who has watched the rise of surveillance in all forms, who proclaimed, “George Orwell may have been an optimist,” in imagining “Big Brother.”

This issue is at the center of global deliberations. The United Nations is working on a resolution for the General Assembly calling upon states to respect—and protect—a global right to privacy.

To explore the future of privacy, we canvassed thousands of experts and Internet builders to share their predictions. We call this a canvassing because it is not a representative, randomized survey. Its findings emerge from an “opt-in” invitation to experts, many of whom play active roles in Internet evolution as technology builders, researchers, managers, policymakers, marketers, and analysts. We also invited comments from those who have made insightful predictions to our previous queries about the future of the Internet. (For more details, please see the section “About this Canvassing.”)

Overall, 2,511 respondents weighed in on the following questions:

> **Security, liberty, privacy online—**Will policy makers and technology innovators create a secure, popularly accepted, and trusted privacy-rights infrastructure by 2025 that allows for business innovation and monetization while also offering individuals choices for protecting their personal information in easy-to-use formats?
>
> **Please elaborate on your answer.** (Begin with your name if you are willing to have your comments attributed to you.) Describe what you think the reality will be in 2025 when it comes to the overall public perception about whether policy makers and corporations have struck the right balance between personal privacy, secure data, and compelling content and apps that emerge from consumer tracking and analytics.
>
> **Bonus question:** Consider the future of privacy in a broader social context. How will public norms about privacy be different in 2025 from the way they are now?

Some 55% of these respondents said "no" they do not believe that an accepted privacy-rights regime and infrastructure would be created in the coming decade, while 45% said "yes" that such an infrastructure would be created by 2025.

Despite this very divided verdict, there were a number of common thoughts undergirding many of the answers. For instance, many of those answering "yes" *or* "no" shared the opinion that online life is, by nature, quite public. An anonymous respondent even went so far to say, "Privacy will be the new taboo and will not be appreciated or understood by upcoming generations." Respondents also suggested that a fluid environment will continue to confront policy makers. Among the common thoughts:

Privacy and security are foundational issues of the digital world

Our question seemed so apt to respondent **Breanne Thomlison**, the founder and president of BTx2 Communications, a marketing and strategies firm, that she predicted there will soon be a new job title called, "Online Public Safety and Corporate Monetization Director." Its functions: to monitor, create, gain, and maintain trust on a global level, as well as manage expectations from each group. "Without this, innovation will not happen," she predicted.

An executive at an Internet top-level domain name operator who preferred to remain anonymous replied, "Big data equals big business. Those special interests will continue to block any effective public policy work to ensure security, liberty, and privacy online."

A promoter of the global Internet who works on technical and policy coordination, wrote, "By 2025, there will be an international consensus among Internet organizations on how best to balance personal privacy and security with popular content and services. The patchwork approach of national privacy protections will be harmonized globally in 2025, and the primacy of security concerns will be more balanced by such an international consensus. In 2025, the public will see the need to reduce the primary focus on security and create a better, workable balance in favor of protection privacy."

People are living in an unprecedented condition of ubiquitous surveillance

John Wilbanks, chief commons officer for Sage Bionetworks, wrote, "I do not think 10 years is long enough for policy makers to change the way they make policy to keep up with the rate of technological progress. We have never had ubiquitous surveillance before, much less a form of ubiquitous surveillance that emerges primarily from voluntary (if market-obscured) choices. Predicting how it shakes out is just fantasy."

An anonymous respondent wrote, "The politics of surveillance and privacy are so broken, particularly when it comes to industry and government interests, that it is unlikely there will be any positive change."

Another anonymous respondent wrote, "There will be a subset of the public rebelling against this surveillance and data-driven society through either withdrawal from the online world or acts of 'civil disobedience' against the powerful."

People require little more inducement than personal convenience to disclose their personal information

Bob Briscoe, chief researcher in networking and infrastructure for British Telecom, wrote, "Lack of concern about privacy stems from complacency because most people's life experiences teach them that revealing their private information allows commercial (and public) organisations to make their lives easier (by targeting their needs), whereas the detrimental cases tend to be very serious but relatively rare."

An information science professional responded, "Individuals are willing to give up privacy for the reasons of ease, fastness, and convenience… If anything, consumer tracking will increase, and almost all data entered online will be considered 'fair game' for purposes of analytics and producing 'user-driven' ads. Privacy is an archaic term when used in reference to depositing information online. Unlike writing a note of secrecy and keeping it safely guarded inside a vault, keeping information hidden and secure online is radically different. Any vault can be ransacked, but imagine the robbers are hundreds of thousands of miles away, invisible and while traceable, takes time and resources the victim may not have. We live in an age where we all feel like rulers to our information, kings and queens of bank accounts, yet we are not; herein lies the problem." Relatedly, **Gina Neff**, an associate professor of communication at the University of Washington, wrote, "People will be increasingly more accepting of exchanging privacy for services and customization, unless advocacy and education efforts are increased now." And **Niels Ole Finnemann**, a professor and director of Netlab, DigHumLab in Denmark, said: "The citizens will divide between those who prefer convenience and those who prefer privacy."

Norms are always evolving, and privacy will certainly change in coming years

Nick Arnett, business intelligence expert, and creator of Buzzmetrics, wrote, "Society's definitions of 'privacy' and 'freedom' will have changed so much by 2025 that today's meanings will no longer apply. Disagreements about the evolving definitions will continue."

Homero Gil de Zuniga, director of the Digital Media Research Program at the University of Texas-Austin, responded, "By 2025, many of the issues, behaviors, and information we consider to be private today will not be so… Information will be even more pervasive, even more liquid, and portable. The digital private sphere, as well as the digital public sphere, will most likely completely overlap."

Rebecca Lieb, an author and an industry analyst for the Altimeter Group, wrote that today's Millennials will be policy makers by 2025: "My optimistic viewpoint is that, with just a bit more time, those who will attempt to balance the interests of personal privacy and business interests will do so from a more informed perspective, legally, culturally, and with a better perspective on disruption."

And a longer-term perspective was offered by **David Ellis**, course director for the Department of Communication Studies at York University in Toronto: "Like so much in online culture… privacy has no end game; the 'right balance' today will not be seen as workable tomorrow."

An arms-race dynamic is unfolding

Peter Suber, the director of a US-based project working for open access to research, wrote, "We can be sure that privacy technology, like encryption, will continue to improve in ease and power—but so will privacy-penetrating technology. It is an arms race today, and I do not see that changing anytime soon. There will always be smart and motivated people on both sides."

An attorney at a major law firm predicted, "The current arms race of privacy between individuals who want it and governments who wish to eliminate it will continue unabated. As cryptography grows stronger, so, too will the ability to break it. As new methods of maintaining privacy are created, the government, particularly the US government, will continue to do what it has done since the days of the Clipper chip—demand back-door access in public, while figuring out how to circumvent it in private… As Google Glass and attendant projects grow, the so-called Internet of Things becomes increasingly aware of literally everything, and as programmers begin jumping on algorithmic schemes to sift, curate, and predict the data, notions of privacy will be considered a fetish. The more data that is captured, the more algorithms will be able to predict, the less privacy we will have, as there will be an assumption that the predictive algorithm is right, and behavior will modify to address actions which have not yet occurred but are likely to a high statistical probability."

Renegotiation and compromise will be a constant in privacy-security policy space

Joe Kochan, chief operating officer for US Ignite, a company developing gigabit-ready digital experiences and applications, observed, "I do not believe that there is a 'right balance' between privacy, security, and compelling content. This will need to be a constantly negotiated balance—one that will swing too far in one direction or another with each iteration… Public norms will continue to trend toward the desire for more privacy, while people's actions will tend toward giving up more and more control over their data."

An entrepreneur and electrical engineer active in ACM and IEEE wrote, "I foresee a minor increase in privacy due to legislation and/or regulation but expect the current tension to continue as innovators find ways to induce people to sacrifice some of their privacy to various compelling (or apparently compelling) applications."

And an anonymous respondent wrote, "Advocacy groups, service providers, large e-commerce companies, Google/Amazon/Facebook/Twitter, secret services, security officers in companies and consultancies, and individual Internet users… are also very much involved. There will be ongoing tension between these groups, and I expect media panics and strategic games."

Other Resounding Themes

It is striking that many in both groups see living a public life online as the new default, though they often made different arguments about whether this would be helpful to creating a widely accepted regime of privacy or a harmful development that would lead to the unstoppable erosion of privacy.

Beyond the broad thoughts listed above there were additional themes often touched upon among the diverse concerns and hopes of those who answered the initial question “no” or “yes.” A large sampling of the thousands of answers received is organized under these themes in the content that follows.

Themes commonly found in the answers of those who say they expect there will not be a widely accepted privacy infrastructure by 2025

1) Living a public life is the new default. It is not possible to live modern life without revealing personal information to governments and corporations. Few individuals will have the energy or resources to protect themselves from 'dataveillance'; privacy will become a 'luxury.'

2) There is no way the world's varied cultures, with their different views about privacy, will be able to come to an agreement on how to address civil liberties issues on the global Internet.

3) The situation will worsen as the Internet of Things arises and people's homes, workplaces, and the objects around them will 'tattle' on them. The incentives for businesses to monetize people's data and governments to monitor behavior are extremely potent.

4) Some communities might plan and gain some acceptance for privacy structures, but the constellation of economic and security complexities is getting bigger and harder to manage.

Themes in responses of those expecting a trusted and reliable privacy arrangement by 2025

1) Citizens and consumers will have more control thanks to new tools that give them the power to negotiate with corporations and work around governments. Individuals will be able to choose to share personal information in a tiered approach that offers varied levels of protection and access by others.

2) The backlash against the most egregious privacy invasions will bring a new equilibrium between consumers, governments, and businesses—and more-savvy citizens will get better at hiding things they do not want others to see.

3) Living a public life is the new default. People will get used to this, adjust their norms, and accept more sharing and collection of data as a part of life—especially Millennials and the young people who follow them. Problems will persist and some will complain but most will not object or muster the energy to push back against this new reality in their lives.

Themes commonly found in the answers of those who say they expect there will not be a widely accepted privacy infrastructure by 2025

Theme 1) Living a public life is the new default. It is not possible to live modern life without revealing personal information to governments and corporations. Few individuals will have the energy, interest, or resources to protect themselves from 'dataveillance'; privacy will become a 'luxury.'

A principal engineer at Cisco wrote, "I would like to eat all I want *and* lose weight, but that trick does not work either." An anonymous respondent wrote, "Privacy rights will be managed by market solutions, with the affluent able to maintain better control of their privacy. Like luxury cars and summer homes, control over private data will be the privilege of winning financially."

Kate Crawford, a professor and research scientist, responded, "The last 10 years have given us a discouraging surfeit of evidence that companies will preference their ability to extract, sell, and trade data than establish simple, easy-to-use privacy protecting mechanisms. In the next 10 years, I would expect to see the development of more encryption technologies and boutique services for people prepared to pay a premium for greater control over their data. This is the creation of privacy as a luxury good. It also has the unfortunate effect of establishing a new divide: the privacy rich and the privacy poor. Whether genuine control over your information will be extended to the majority of people—and for free—seems very unlikely, without a much stronger policy commitment. Optimistically, people are better informed about how their data can be used to discriminate against them and demand greater security, privacy, and access to due process. Pessimistically, people may want those things, but they have no real power to get them."

The executive director of a nonprofit that protects civil liberties online responded, "I do not think policymakers or technology innovators have the incentives to create a privacy-rights infrastructure, but even if they did, I do not believe governments will stop mass surveillance. It breaks my heart, but I do not think we are going to get this cat back into its bag. Sadly, I think individuals will get used to the fact that mass surveillance exists and will not expect privacy by 2025."

Bryan Alexander, technology consultant, futurist, and senior fellow at the National Institute for Technology in Liberal Education, wrote, "Too many state and business interests prevent this. Governments, from local to national, want to improve their dataveillance for all kinds of purposes: war fighting, crime detection, taxes, and basic intelligence about economics and the environment. Companies badly want data about customers, and some base their business models on that. I do not see this changing much. Citizen action is probably the best option, much as it was for crypto in the 1990s. But, I do not see that winning over governments and big business… In the United States, both political parties and the clear majority of citizens cheerfully cede privacy."

Clifford Lynch, executive director for the Coalition for Networked Information (CNI) and adjunct professor at the School of Information at the University of California-Berkeley, wrote, "Government and industry have aligned and allied to almost totally eliminate consumer and citizen privacy. This will not be allowed to change at scale—it is too convenient and too profitable for all parties involved. Today, it is almost impossible for consumers to opt out of the corporate side of this data collection and tracking because it is so pervasive, and, in 2013, the stunning scale of the government side of data collection has become clearer, as well as the government's willingness to either purchase or legally demand data collected by corporations that the government cannot collect directly. You will see a small fringe of technically savvy people who will try to continue to deploy technology to protect some privacy for some purposes, but this will be small and periodically attacked or placed under particularly intense surveillance. You will also continue to see the government try to punish corporations who try to side with their customers, and reward corporations who are helpful to government objectives."

Cathy Davidson, co-director of the PhD Lab in Digital Knowledge at Duke University, and co-founder and principal administrator of the MacArthur Foundation Digital Media and Learning Competition, wrote, "I fear the coming of walled Internets, where there is security but also pay walls—and the security is partial. The relationship of privacy, security, and openness is not resolved, and I fear it will not be done in a way that allows for openness in the future."

An anonymous respondent replied, "There will not be a trusted privacy-rights infrastructure allowing for individual choice… The overall public perception will be that the right balance has been struck, as privacy will be only a concern for cranks. Employer concerns about employee behavior off-hours will fade, as a generation will have come of age with shared party photos and selfies, and will reject current norms requiring either privacy or sanitized private behavior—a concept which will have little meaning."

Theme 2) There is no way the world's varied cultures, with their different views about privacy, will be able to come to an agreement on how to address civil liberties issues on the global Internet.

Alice Marwick, researcher of the social and cultural impacts of social media and author of *Status Update: Celebrity, Publicity, and Branding in the Social Media Age*, wrote, "It will be quite difficult to create a popularly-accepted and trusted privacy rights infrastructure. This is for a number of reasons. First, countries, regions, and cultures differ in their approaches to privacy. For example, the United States, European Union, and Canada all have different approaches to online privacy and what constitutes acceptable data collection."

John E. Savage, chair in computer science at Brown University and a fellow of the IEEE and the ACM, wrote, "A secure, accepted, and trusted privacy-rights infrastructure on the Internet, at the global scale, is impossible for the foreseeable future. For too many large nations a tension exists between state security and privacy rights. They will not sacrifice the former for the latter—a position that is not going to change unless revolutions occur, which is highly unlikely in the more developed nations. In democratic countries, bilateral and multilateral agreements respecting the privacy of citizens for commercial purposes are likely to be developed. It is highly unlikely that nation states will forswear invasion of individual privacy rights for national security purposes."

Henning Schulzrinne, an Internet Hall of Famer, technology developer, and professor at Columbia University, observed, "Each country is likely to make very different trade-offs, with continued inaction and stalemate in the United States likely. The influence of policy makers and innovators is limited; most of the privacy issues are beyond the direct influence of either, unless one would call advertising-driven companies 'innovators.' Given diminishing returns on traditional advertising and general industry concentration in many areas (from airlines to telecom), there will be increased pressure to gather more data on consumers—i.e., to price-differentiate offerings in near-monopoly settings. There are likely to be limited offerings for privacy protection (i.e., pay email services), but they are likely to be much less convenient or more costly and thus limited to the sophisticated 1% of the Internet population. The question presumes that there is such a public norm today. My perception is that most people do not think deeply about these issues and do not have good ways to understand what exactly is being done. In particular, the notion that PII [personally identifying information] data is and will be available, sometimes by necessity, but that processing and usage of that data are hard to see, make establishing norms difficult."

There's also a matter of the cultural differences between Internet business interests and governments' interests. An anonymous respondent replied, "I have difficulty foreseeing policymakers and corporations coming to agreement on privacy issues when there is little current agreement. Also, security is clearly not a high priority for corporations, and there seems to be little effort on the policy side to compel them to take it seriously. Content and apps will take care of themselves. I also do not see privacy becoming a major norm without some very major, personally affecting event. There are already tools that do not get taken advantage of to help with privacy, and people make little effort to change their behavior to promote privacy."

Theme 3) The situation will worsen as the Internet of Things arises and people’s homes, workplaces, and the objects around them will ‘tattle’ on them. The incentives for businesses to monetize people’s data and governments to monitor behavior are extremely potent.

An anonymous respondent wrote, “As long as greed plays a role in our society, it will always be dominant in how policymakers and corporations treat the individual. There will be less privacy and more access to everything, including your DNA.”

Vickie Kline, an associate professor at York College responded, “Medical privacy will be the most paradoxical; we will have unprecedented data at our fingertips to make proactive decisions about our health, but the objects around us, and even our clothes, will tattle in real-time about the choices we make. We have to work towards security, liberty, and privacy online, but government and corporate intelligence and hackers will always keep us outside of the comfort zone. I wonder if the expectation of privacy as a right will gradually fade as people experience less actual privacy in their lives.”

Bill Woodcock, executive director for the Packet Clearing House, responded, “The year 2025 is 11 years away. Over the past 11 years, both public expectations and the reality of privacy online have degraded substantially, and I do not see any net reversal in the direction of that trend. There are certainly bits of progress here and there, but I imagine that in 2025 the same incentive structures will be in place: corporations will still see immense benefits to correlating and de-anonymizing PII [personally identifying information], politicians will still either be in the pockets of lobbyists or pursuing their own unrelated agendas, and individuals, *en masse*, will still be too clueless to protect their own data. A new generation will have come of age at that point—people who have dealt with these issues since childhood. If we look at other generations that have come of age in eras of new technology (the automobile, television, ubiquitous advertising, etc.), we see a greater and more pervasive sophistication in parallel with ever-greater volumes of change. Following that logic, PII will be collected even more than now—literally, at every turn, in every public place, any time one uses most technology products; but, users will have a general awareness that that's the case, and most users will take some steps to manage or mitigate it.”

A self-employed software designer and policy researcher wrote, “Policymakers and private industry will do what it takes to convince consumers that they are reasonably secure, while also continuing to permit industry to exploit consumer information (at individual and collective levels) in new ways for profit and for purposes that suit state ‘needs’ (these needs being determined by the dominant value system, which usually is framed in terms of promoting free market-based 'innovation,’ state security, taxation, etc.). If we are speaking about so-called Western states: the young people today will be adults. They already have too much control as the main consumers of technology and as the voices that industry caters to and tries to manipulate through 'identity empowerment.' At that point, they will be the value definers. They already have completely different concepts of personal identity, privacy, etc... We can expect that 'private' will not be an adjective that commonly precedes 'space' or 'life,' and that public disclosure and exposure of intimate life or economic details may not even be described as such, that associating corporate brands with personal identities will continue to perpetuate until people do not even recognize branding as branding (actually, that is already the case — cf. 'sent from my iPhone' and logos on clothing). Even physical 'private property' may become more exposed and less private, as we increasingly turn to home automation technologies to remotely control our door locks, IP security cameras, lights, alarms, etc."

Kalev Leetaru, Yahoo fellow in residence at Georgetown University, wrote, "While… people publicly discuss wanting more privacy, they increasingly use media in a way that gives away their privacy voluntarily—for example, broadcasting their location via phone GPS when posting to social platforms, photographing their entire lives, etc. People seem to want to be famous, documenting their lives to the most-minute detail, in ways that would have been unheard of to a past generation. Moreover, each time a major social platform reduces privacy even further, there is a roar of public backlash and promises that people will leave *en masse*, but no one actually leaves the platforms, and in fact, more sign up. Thus, people are not voting with their feet. Companies have no incentive to increase privacy, which reduces revenue possibilities in terms of selling advertising and products based on identity and desires… For my detailed thoughts on this, see the chapter Tony Olcott and I wrote for a volume on changing norms on privacy."

Theme 4) Some communities might plan and gain some acceptance for privacy structures, but the constellation of economic and security complexities is getting bigger and harder to manage.

A pioneering academic computer scientist from Princeton University wrote, "I do not expect a comprehensive solution in this area, nor one that makes everybody happy. These will continue to be contested areas, with different parties using legal, political, and technological means to advance their interests. We will have a stronger and better-defined notion of how to protect vulnerable populations such as children. We will have a better-defined set of social norms around the use of private information. We will have a better understanding of how 'pseudonymous' information about behavior and relationships affects people's privacy interests."

Alex Halavais, an associate professor of social and behavioral sciences at Arizona State University, predicted, "There will be multiple such infrastructures within smaller communities, but nothing even approaching broad acceptance. The problem being addressed is a significant one, but efforts thus far have proven to be too complex to navigate effectively. If history is any guide, concerns over the NSA incursions and related breeches of privacy will be too short-lived to create the impetus for real change. Perhaps, however, we may see a slight increase in the availability and use of strong encryption tools. I suspect our language around privacy may evolve. The word, on its own, is too broad to encapsulate the broad range of concerns: everything from marketers stalking Web traces to state use of CCTV [private video surveillance]. Until the issue of 'privacy' is appropriately segmented, we will have a tough time either talking about it or addressing it."

A distinguished engineer, working in networking for Dell, wrote, "There are too many challenges to maintaining privacy and providing security at the same time. In some ways, they are conflicting goals. People will become more aware of the lack of privacy, but, if at all, there will be less of it."

Brian Butler, a professor at the University of Maryland, responded, "Within the United States, we have already largely decided to privilege the corporate use of personal data for 'utilitarian' purposes, to the point where is it difficult to see what could happen in the next twelve years to shift this… I suspect that there is a developing privacy 'divide'—one group (the same group that 'wins' in the case of the digital divide) will have the technical and literacy skills to manage privacy—but because of this, they will be cavalier with this (hence the 'privacy is outdated' idea). On the other hand, individuals who lack the skills, ability, or time to manage this complex issue will be increasingly subject and resigned to less and less privacy and control. One thing that we have to remember is that it is hard to figure out the institutional and technical aspects of privacy if you are working two or three high-effort jobs and trying to stay awake."

A principal engineer with Ericsson wrote, "The real danger here is not just the further invasions of privacy, but also the increasing impression that people can have their behavior modified 'for the good' through these means. The danger comes when people move from attempting to modify behavior for commercial reasons to trying to modify behavior for political ones, by examining what makes people think a certain way or prompts them to take action or causes them to believe certain things en masse. In fact, it can be argued that we are already seeing this sort of thing take place, with large data analytics firms, such as Google and Facebook, getting deeply involved in politics. The Internet will go in one of two directions: either people will reject behavior modification through data mining en masse, or we will become so habituated to having our behavior modified through data mining that we will not even consider the consequences by the time 2025 rolls around. It is hard to tell which direction things are going to go at this point, but if it is the former, the backlash against technology in general is going to be greater than we imagine, I think. By 2025, privacy will be a moot issue, most likely. Instead, we will be focusing on the moral issues behind using proven techniques of behavior modification, if there is any debate at all."

Themes in responses of those expecting a trusted and reliable privacy arrangement by 2025

Theme 1) Citizens and consumers will have more control thanks to new tools that give them the power to negotiate with corporations and work around governments. Individuals will be able to choose to share personal information in a tiered approach that offers varied levels of protection and access by others.

Doc Searls, director of ProjectVRM at Harvard University's Berkman Center for Internet & Society, wrote, in part, "There will be a privacy rights infrastructure in place long before 2025. I believe it will materialize within the next three to five years… [It] will come from new technological approaches that enable individuals and organizations to operate in full privacy without fear of surveillance. These approaches will be distributed, rather than centralized… Key to our emerging privacy-creating system will be the ability of individuals to assert their own terms, policies, and preferences in dealings with others, including companies and governments—and for equal consenting parties to work out norms that do not require intervention or control by large companies or governments… The end state will be one in which individuals will enjoy far more control of their personal data, and privacy in general, than they do today, and that will be good for business."

David Weinberger, a senior researcher at Harvard's Berkman Center for Internet & Society, observed, "They will because they have to. Unfortunately, the incentives are unequal: There is a strong incentive to enable strong privacy for transactions, but much less for enabling individuals to control their own info. So, of course, I do not actually know how this will shake out. I assume we will accept that humans do stupid things, and we will forgive one another for them. When your walls are paper, that is what you have to do."

Jim Hendler, an architect of the evolution of the World Wide Web, and professor of computer science at Rensselaer Polytechnic Institute, wrote, "There will be significant progress in this area, although choosing 'Yes' was the only way to go [in answering the survey question] I think there will still be many privacy issues continuing to evolve. People will be more aware of how their information is being used, who is allowed to collect it, and what redress they have when there are violations; however, the amount of personal information that will be available, and the potential for abuse, will also grow rapidly. Thus, I think there will still be many issues to be resolved. The basic notion of what 'privacy' means will have to change in terms of various rights."

JP Rangaswami, chief scientist for Salesforce.com predicted, "I suspect that, in times to come, privacy rights will begin to look like the 'Four Drivers' in the Nohria-Lawrence 'Driven' model: the right to 'defend' private information; the right to 'bond,' or share, it; the right to 'learn,' or gain insights, from it; and the right to 'acquire,' or own, it. As we learn more about the value of personal *and* collective information, our approach to such information will mirror our natural motivations. We will learn to develop and extend these rights. The most important change will be to do with collective (sometimes, but not always, public) information. We will learn to value it more; we will appreciate the trade-offs between personal and collective information; we will allow those learnings to inform us when it comes to mores, conventions, and legislation."

An anonymous survey participant who works in the US executive branch, commented, "Governments will have to learn to do more as public-private partnerships and active engagement with citizens to do crowdsourcing. The nation-state model is already being challenged; issues span borders and across sectors. The infrastructure will require transparency among governments as a trusted partner—but also recognizing that not all data can or should be made open. We will be trusting machines more; we will have our digital device (a smartphone, an embedded device in us, etc.) interface with systems to pre-negotiate what information we will and will not share. End-user licensing agreements will be machine-to-machine."

David Bollier, a long-time scholar and activist focused on the commons, responded, "There are feasible alternatives already being developed, such as by ID3 in Boston. Here are two pieces that shine a light on this area—one by Doc Searls (summarizing Fred Wilson) … and the other, my own piece (with John Clippinger) on 'authority and governance' as the next big Internet disruption… The existing structures are highly unlikely to yield the infrastructure that we need—but an alternative system is still possible, if only because the latent network value of doing so is so huge. Assuming the infrastructure development pathway mentioned above comes to pass, privacy norms will be affirmatively structured and managed, mostly by tech systems amenable to meaningful human control, rather than 'taken for granted' as a natural social reality. This will require that ordinary individuals be empowered to protect their privacy rather than relying upon government surrogates to do so. We have seen how government is far too beholden to national security and incumbent corporate interests, and too centralized and bureaucratic in a networked age, to be an effective watchdog and implementer of larger collective concerns."

Theme 2) The backlash against the most egregious privacy invasions will bring a new equilibrium between consumers, governments, and businesses—and more-savvy citizens will get better at hiding things they do not want others to see.

Peter McCann, a senior staff engineer in the telecommunications industry, responded, "There is a large momentum toward increasing privacy protections on the Internet in the wake of the Snowden revelations. A new infrastructure of pseudonymous communication and transaction will be created over the next few years, with robust privacy protections built in. These protections will take the form of a distributed database, where cooperation among many entities will be required to reveal personal information about a user, making the secret warrant useless, and warrantless intrusions on privacy impossible. There will be a broad expectation of privacy unless social norms are violated in an obvious way, in which case, the offender will be rapidly tracked down and sanctioned."

Christian Huitema, a distinguished engineer with Microsoft, replied, "I expect many efforts to make the Internet more robust to attacks, including attacks by secret services. But, I do not think that privacy rights can be protected by an 'infrastructure.' They can, on the other hand, emerge from competition, i.e., 'free as spy' services competing with some 'pay and trusted' services. People are going to learn what to share and how to share it. We see that, already, among the young generation. Project a neat, public image, and keep your personal stuff actually private."

Tom Standage, digital editor for The Economist, wrote, "As with financial regulation, privacy regulation makes progress as a result of regular crises. Technology firms (and security agencies) will repeatedly over-reach and then be brought into line by consumer pressure/boycotts and new regulations. In this way, we will discover where people would like to draw the line when it comes to paying for Internet services using personal data. I think this trade-off will become more explicit: use this service free by giving us access to your data, or pay for it. For a long time, it has been assumed that Gen Y-ers have a different attitude to privacy and are more inclined to make everything public; the success of Snapchat this year suggests otherwise. As people get older, they worry about this more. It is possible to have mass take-up of publishing tools, while also agreeing that it makes sense to keep some things private."

Theme 3) Living a public life is the new default. People will get used to this, adjust their norms, and accept more sharing and collection of data as a part of life—especially Millennials and the young people who follow them. Problems will persist and some will complain but most will not object or muster the energy to push back against this new reality in their lives.

Stewart Baker, a partner at Steptoe & Johnson, a Washington law firm, wrote, "Security is a pain in the butt, a major inconvenience. It also hampers innovation. We will not give up convenience and innovation without living through a disaster. Almost everything we are shocked and worried about—including all the things we are saying the government should never do—will be commonplace by 2025. And, it will not really bother us that much. Privacy is the most malleable of expectations."

Ben Shneiderman, professor of computer science at the University of Maryland, wrote, "There will continue to be pressures for increased security, liberty, and privacy, but there are powerful forces working to enable businesses to track behavior, as well as government to monitor activity. While I am not fearful of dystopian futures, doing things on the Internet will be much more like being in public than being in the protected privacy of your home. Recognition of the Internet as a public, and not private, space will be more widespread. There will still be scams, pornography, stalking, etc., but the worst cases will be stopped, and Internet benefits will outweigh threats. Premium services that offer more privacy will be valued."

Marjory Blumenthal, a science and technology policy analyst, wrote, "There is a lot of pressure to do something—now. So, one can expect work on an infrastructure that will be relatively secure. Whether it will be popularly accepted—that is harder to say, since skepticism has skyrocketed. People will become more aware of the tradeoffs, which will drive an evolution of norms. They will also have become more sophisticated about choices regarding disclosures they make, exercising finer-grained control—in part because there will be more technical support for doing so—and there will also have been evolution of the legal and regulatory framework."

Jeff Jaffe, CEO for the World Wide Web Consortium, the standards-setting body for the Web, wrote, "Today's policy makers have difficulty in making basic policy tradeoffs in existing areas such as spending and taxes. They are not ready to step up to these new complex issues. The generation of teenagers growing to adulthood will have different norms for privacy than today's adults."

Jonathan Grudin, principal researcher at Microsoft Research, responded, "There is an inevitable tension between potential commercial exploitation of personal information by businesses, including those that are well-intentioned, and the desires of some individuals. Businesses will always be motivated to push infrastructure boundaries, whatever they are. In fact, the more work we invest in developing a framework that seems balanced, the more a business can find grey areas, workarounds, and loopholes in good conscience. Young people are more used to a world with cameras everywhere. They spend more time online and identified. The older generation developed behavioral habits that assumed a degree of privacy that young people have not experienced. What oldsters would have to give up, young people will not miss. In 2025, more of the population will have grown up in the new world, so concern about privacy will decrease and perhaps shift in emphasis. Of course, the dwindling ranks of dinosaurs may not see things much differently than they do now."

Privacy is a passing artifact of the industrial age: One further insight emerged in several answers—that privacy might gradually fade and become recognized as a social construct of the industrial age. Several noted that the rise in urbanization that came once factories were built moved people from villages where they enjoyed little privacy into social settings where privacy among the masses could be achieved. Now, the pervasive social connectivity and awareness afforded by digital technology could be returning people to that village-like environment.

One version of that thought came from **Bud Levin**, a futurist, and professor of psychology at Blue Ridge Community College in Virginia: "Increasingly, and gradually, people will realize that privacy, anonymity, confidentiality, secrecy, and similar constructs of the industrial age, are giving way to ubiquitous transparency. Consider how we might behave when we know that everything we do is or could easily become headline news. Privacy laws will become more obviously incompatible with normal behavior. They will be trying to push back the ocean. That is likely to generate increasing contempt for government." And **Vickie Kline**, an associate professor at York College responded, "Government and corporate intelligence and hackers will always keep us outside of the comfort zone. I wonder if the expectation of privacy as a right will gradually fade as people experience less actual privacy in their lives."

One thoughtful writer synthesized a variety of "yes" and "no" themes and put them in the context of a future in which the Internet of Things, more powerful artificial intelligence, big-data analytics, and other factors combine to learn and infer things about individuals.

> **Barry Chudakov**, founder and principal of Sertain Research, wrote, "By 2025, we will begin to define an emergent problem: any secure, popularly accepted, and trusted privacy-rights infrastructure must balance transparency with intrusion, and as we develop subtler and more powerful technologies that become ever more intrusive, we will realize how difficult this is.
>
> We will continue to monetize watching and tracking; cameras and recognition technologies will create 'everyware.' As we do, rights and choices will collide; we will struggle to satisfy forces of personal privacy, secure data, compelling content, and tracking and analytics. This entails 'thinking fast and slow'—and in a decade, we will still struggle with statistical (probability) thinking versus quick-get thinking. We will be challenged to not fall in love with our invasive tracking, watching, and predictive technologies and their beautiful data displays, marketed in easy-to-use formats.
>
> We will slowly realize the inherent conflicts between our data summations and the reality they are summarizing. Privacy will ostensibly be hidden behind this mask of abstract data; it may well be hidden by the seductive insights of simulation. This will create both intense interest and equally intense insecurity about personal information. As monitoring and statistical tools enable us to abstract behaviors to norms, trends, and

predictions, it is inevitable, given our inclination to turn information into more information, which we will engage with the abstraction as if it were real—as if it were the concrete thing it is abstracting. This can lead to inaccurate, even wildly distorted, perceptions, as we saw in the credit default swaps of the 2008 Wall Street meltdown.

A healthy tension will arise: many of us will separate the thing (whatever it is we are tracking and analyzing) from the data abstraction; but equally, many others will not—either because they cannot (they are not trained or equipped to do so) or because they do not want to. Yes, more average persons will start to understand opt-in data capture and monitoring protocols that enable tracking and analytics. But, when our gestures and bodily identifiers—gait, ear lobes, eye movements, faces, emotional responses, or behaviors and choices—are the content of that tracking and analysis, we ourselves become the abstraction.

I do not believe that, in a decade, we will have resolved all the quandaries of this new reality. We will become smarter about it, but we will also be more conflicted. This abstraction of our actions and inclinations is bedeviling because privacy and tracking and analytics should be at odds with each other; they are strange bedfellows, and we are better served by understanding that tension among them is healthy. Further, once our movements and choices and behaviors are captured, digested, and brought to some enhanced understanding, we may know more about certain actions.

But, in our delight over data and analytics, will we match that with enhanced empathy for and understanding of each other? The public will slowly come to realize that privacy is what we are left with after our technology enables discovery of what we want to know. Do we want to know your actions, your behaviors, and your pathway through the city or store? Do we want to know your face, your emotions, and your demographic data? Do we want to know if you were in a certain place at a certain time? Such knowledge, and much more detailed knowledge of behavior patterns, trends, and predictions, will define privacy in the broader social context.

Like the remainder in a division problem, privacy is the problematic ‘answer’ after we divide our lives by the technology to watch and measure those lives. Knowledge is power (and profit) for some, and it is so-called ‘security’ for others. The struggle with the balance between the far-reaching knowing of technology and keeping our identity intact is the future of privacy in a broader social context. We now think of privacy as the ability to keep our information to ourselves. By 2025, we will expand that to include the ability to keep our identity and natures from being invaded by other techno-forces, as well as to keep our identity in line with our intent and volition.

The desire for fame has already put identity up for sale; as our technologies enable us to know virtually anything about others, privacy will become a commodity. It will be sold to the highest bidder; privacy will become the offshore bank account of identity. Regular people will be transparent; those who can pay for opacity will do so via new services and business models. While I think this will eventually be available to more than just the wealthy, we will not have sorted this all out in just a decade, and so, privacy will be available to those with the fattest bank account."

Above-and-Beyond Responses: Part 1

A variety of views in regard to this issue are reflected in these big thinkers' imaginings of what may happen by 2025.

'Social punishment may have to be accompanied by legislation'

Vint Cerf, Google vice president and chief Internet evangelist, responded, "The public will become more sophisticated about security and safety. Corporations and service providers will feel pressure to implement practices including two-factor authentication and end-to-end cryptography. Users will insist on having the ability to encrypt their email at need. They will demand much more transparency of the private sector and, especially, their governments. Privacy conventions will evolve in online society—violations of personal privacy will become socially unacceptable. Of course, there will be breaches of all these things, but some will be accompanied by serious social and economic downsides and, in some cases, criminal charges. By 2025, people will be much more aware of their own negligent behavior, eroding privacy for others, and not just themselves. The uploading and tagging of photos and videos without permission may become socially unacceptable. As in many other matters, the social punishment may have to be accompanied by legislation—think about seat belts and smoking by way of example. We may be peculiarly more tolerant of lack of privacy, but that is just my guess."

The key will be defaults: Individuals will control their personas or be controlled

Marc Rotenberg, president of the Electronic Privacy Information Center (EPIC), said, "There will be many contentious battles over the control of identity and private life. The appropriation of personal facts for commercial value—an issue that emerged with Google's 'shared endorsements' and Facebook's 'sponsored stories'—are a small glimpse of what lies ahead. The key will be the defaults: either individuals will control their online persona or it will be controlled by others."

'We will get used to an open society; answer surveillance with 'sousveillance''

Futurist **David Brin**, author of a highly respected book on the future of privacy, *The Transparent Society*, wrote, "See my book, *The Transparent Society*. We will get used to an open society; answer surveillance with 'sousveillance.' It matters less what others know about us than what they can (not) *do* to us. To control that, we must look back at the mighty and watch the watchers. The question implies that the only solution will be to create some paternalistic, unified structure to control and parcel out information. Even if it is designed by honest and skilled people, this approach cannot work. Can you name for me *one* example when that ever worked in a reliable way? How many supposedly reliable systems and databases leak (surprise!) every year? There is a better way."

Dynamics of security and privacy 'mired in ugly politics and corporate greed'

danah boyd, a research scientist for Microsoft, responded, "What you're suggesting sounds like a fantasy. I expect the dynamics of security and privacy are going to be a bloody mess for the next decade, mired in ugly politics and corporate greed. I also expect that our relationship with other countries is going to be a mess over these issues. People will be far more aware of the ways that data is being used and abused, although I suspect that they will have just as little power over their data as they do now."

'Norms and laws are often syncopated with innovation in technology'

Jeff Jarvis, director of the Tow-Knight Center at the City University of New York, wrote, "Just as with the introductions of many technologies before—the telephone, the portable camera, even the Gutenberg press—society renegotiates its norms to catch up with progress, as well as to recognize the benefits innovation can bring, while also protecting against its risks… Norms and laws are often syncopated with innovation in technology. Now, with the Internet, we are once again renegotiating our norms around privacy and public-ness. Thanks to Edward Snowden, I hope we will also soon renegotiate our privacy laws and governmental norms. I do believe that the public, business, and government can work to maximize the benefit of the Net, while also minimizing danger. Of course, there is nothing to guarantee they will. Government, threatened by the redistribution of power brought by the Net, could succeed in claiming sovereignty over it, throttling its freedoms. Business could overstep its trust with consumers and bring regulation into place. Media could succeed in breeding moral panic—technopanic—over anything that could go wrong. But, I hope that enlightened self-interest will prevail…Vint Cerf, co-inventor of the Net, and evangelist for Google, said recently that privacy might be a historical anomaly. That is the kind of blunt, albeit factual talk that can drive a corporate public relations person to drink. Still, he is right that privacy is, by various accounts, a relatively recent invention, born of hallways (allowing people to close doors on their activities) and cities (letting individuals become lost in the crowd). Yet at base, privacy is what it always has been: that which we keep to ourselves, in our heads, unspoken, except perhaps to intimates we trust (though what we tell them is then public to that extent). That is still the case, and always will be, no matter what medium we use to share…"

A tiered-system might have *Privileged*, *Private*, *Business*, *Public* levels

David P. Collier-Brown, a system programmer and author, predicted that by 2025, "I expect at least four levels and categories. The levels are: *Privileged*—communications with my doctor, lawyer, Member of Parliament, etc. *Private*—things I share only with selected correspondents. *Business*—things I share with particular businesses, with protections against aggregation. *Public*—things I share with everyone. The categories are orthogonal to these, and are identified uniquely as me. I sign *these* with the private key I have registered with Elections Canada–identified for financial purposes. I sign *these* with a private key that has a credit card; the card issuer knows who I am, while others do not. A pen name and age is published for each of *these*, but it may not be strongly linked to me. Right now, I use different middle initials to distinguish self-identifications; to you, I am David P. Collier-Brown; to American Express, I'm David A. Collier-Brown—unique—lots of pen-names, avatars and nicknames, partially trackable. I expect people to be less concerned about some areas, like pictures, but more concerned about others, like vendors doing cross-matching. Pictures of nude sunbathing will be about as embarrassing and threatening as naked baby pictures. Ads will have 'just for me' categories, but nasty snooping by advertisers will result in picket lines and class-action suits."

'From the state to the private sector, surveillance won'

Howard Rheingold, a pioneering Internet sociologist and self-employed writer, consultant, and educator, responded, "When I and others wrote about the ways technologies could enable a surveillance-dataveillance state, as early as the 1990s, few Americans really seemed to care. We could foresee that bridge and freeway transponders, credit cards, closed-circuit video cameras, linked via the Internet, with millions of bits of individually insignificant personal information compiled into dossiers by powerful computers, could provide the infrastructure for unprecedented surveillance… it did not take a prophet to foresee those events. After 9/11, massive US government overreach was rubber-stamped by Congress and accepted by citizens. A huge security bureaucracy was set up. When Admiral Poindexter proposed 'Total Information Awareness' (the TIA program), public outcry shut down the proposed campaign; yet, decades later, when Edward Snowden's leaks revealed that the NSA had gone ahead with an even more far-reaching program, there was neither widespread citizen protest, nor significant Congressional resistance. At the same time, the most powerful growing sector in an otherwise war-weakened US economy, online media—from Google, Amazon, and Facebook on down to every ad-supported Web enterprise—developed a powerful business model based on the same kind of dossiers. From the state to the private sector, surveillance won. At the time of this writing, Google Glass and other surveillance-capable, Web-connected wearables have not been unleashed. It is impossible to tell how people will react to the presence of multiple strangers in almost every public situation, equipped to capture still images and stream video—and also equipped with facial-recognition capabilities. Citizens will join the state and digital businesses in the surveillance game. Privacy is a social construct—for example, until central heating, most people in most houses slept in the same room; in Japan, for centuries, walls were made of paper. Ask any teenager about his or her 'Facebook-stalking' habits. Privacy has already changed."

'Everyone will expect to be tracked and monitored' for services, safety'

Hal Varian, chief economist for Google, wrote, "We will have some sort of usable infrastructure by 2025, but it will be painful getting there. People will be comfortable sharing personal information with organizations because those organizations will be regulated and audited about their practices. There is no putting the genie back in the bottle. Widespread sensors, databases, and computational power will result in less privacy in today's sense but will also result in less harm due to the establishment of social norms and regulations about how to deal with privacy issues. By 2025, the current debate about privacy will seem quaint and old-fashioned. The benefits of cloud-based, personal, digital assistants will be so overwhelming that putting restrictions on these services will be out of the question. Of course, there will be people who choose not to use such services, but they will be a small minority. Everyone will expect to be tracked and monitored, since the advantages, in terms of convenience, safety, and services, will be so great. There will, of course, be restrictions on how such information can be used, but continuous monitoring will be the norm."

Facial-recognition expanding; lack of publicness will seem anti-social and creepy

Judith Donath, a fellow at Harvard University's Berkman Center for Internet & Society, responded, "A big inflection point will be face-recognition. Today, when we meet a new person, we are likely to do a search on their name, often finding out some surprising hobby or other details, perhaps a lengthy blog history, plus the expected professional information. But, the people we see on the street, in the subway, across the restaurant—they remain strangers, enigmatic. Face recognition will change this. We will be able to put a name to a face—and all the data attached to that name. For the citizen of that future world, it will seem strange and unsettling to think that in the past people walked, sat, and ate amidst crowds of unknowable strangers. It will seem dangerous—one of the first apps that will make use of this technology will alert us to registered sex offenders and paroled felons in our midst—and dull. (Today if someone catches your attention, you muse a bit about him or her, and then move on. There is no connection. Tomorrow, you can delve into whatever personal traces they have online.) This will cause a big shift in how we think of privacy and the norms around making information about ourselves public. Today, if someone chooses to have a very low online profile, this has little effect on how we think of him or her face-to-face. But, in this future, that will start to seem anti-social and a little creepy. There will be much more pressure to have such a data presence—and to carefully cultivate it."

Exhibit A for the transparent future: My own life

John Lazzaro, a research specialist and visiting lecturer in computer science at the University of California-Berkeley, wrote, "The reality in 2025 will look like my own reality today. As an employee of a California public university, my salary is public information, and websites exist to let you search for my salary. When I officially teach a class, statistical summaries of student reviews are publicly available online, and I do not have the ability to take them down. Google Scholar lists the number of references for every paper I have published over the past 25 years, which is a common proxy for research impact. The IETF has a meticulous record of every document draft and mailing list email about the RFCs I have authored, which gives a microscopic window on how I work on a technology problem. This level of disclosure is a feature for me, not a bug. Anyone who is curious about who I am professionally can invest a few minutes in Google searches and decide for himself or herself. It is a more honest portrait than what you will find on a website like LinkedIn. And so, I think it will become the norm by 2025."

Maybe a 'Privacy Chernobyl' will change things, but don't count on it

John Markoff, senior writer for the Science section of the New York Times, responded, "I have been writing about privacy, security, and computer networks since the late 1970s. The trend is decidedly away from individual privacy, as well as away from online security. We are on our way to the 'Panopticon.' Conceivably, a 'Privacy Chernobyl' might alter this, but I do not believe the Snowden materials will. I believe that a decade is an infinite period in terms of Internet time. Too many things are possible, and anything we say today would be largely speculative. I am struck by the fact that there is such a gulf between the European and US privacy norms. I believe this is because of World War II. When the Nazis entered Paris, the first thing they did was head for the phone directory."

'The drift toward less privacy will only be reversed if there is a perception that privacy concerns are interfering with commerce'

David Clark, a senior research scientist at MIT's Computer Science and Artificial Intelligence Laboratory, noted, "We will have this in a fragmentary way, but it will not have the character of 'infrastructure.' … The European Union has more of a tendency to address issues like this top-down; the United States seems to work bottom-up. Privacy rights will differ in different contexts—some will be more robust than others. That is why I do not believe that the outcome will seem like 'infrastructure.' The drift toward less privacy will only be reversed if there is a perception that privacy concerns are interfering with commerce. Privacy is a residue left over after concerns about security and commerce are satisfied (this thought is not original to me, but I do not remember who said it). There will be a swing back from the total voluntary disclosure we see today on sites like Facebook. What we will see is a more nuanced way for people to deal with their different friends and colleagues, with more expressive ways to control what is shared. But, the pressures for Big Data tracking will continue to erode our expectations of what is known about us without our explicit disclosure."

'Americans have happily sacrificed their privacy and will continue to do so'

Paul Saffo, managing director at Discern Analytics and consulting associate professor at Stanford University, wrote, "The opposition to privacy erosion is broad and diffuse, while the proponents of privacy-eroding systems are narrow and focused. Further, while Americans claim to care about privacy, they care even more about convenience. Americans have happily sacrificed their privacy over the last several decades, and will continue to do so, even as they complain. Privacy has already shifted from being a right to a good that is purchased. Privacy-as-good will continue to advance and become the 2025 norm."

'In 2025, we will have a post-Facebook and post-Google world'

Marcel Bullinga, a technology futures speaker, trend watcher, and futurist, wrote, "A trusted infrastructure *needs* to be created in order to prevent massive fraud and massive public distrust in online transactions, and in online life, in general. We have to reinvent the entire Internet as we know it, shifting power from a few American tech companies to the individual who creates, and therefore owns, the data. We need to create a personal dashboard, a safe haven, for every individual's dossiers, transactions, money, and profiles. In this dashboard, you could set your privacy and communications settings (from 0 to 100%). All of this will create a big struggle about the question: Who owns (my) data? My 2025 statement: In 2025, we will have a post-Facebook and post-Google world. We will have new business models in which facilitating data is more lucrative than owning data. Providers who refrain from owning their customers' data and stick to facilitating the owner in handling their data in a trusted way will win. This means Google and Facebook will lose. If we do not make this transition, we face a privacy and fraud nightmare in which our lives are dominated by a few global tech companies… There are two opposite trends: first, we will adapt to 100% transparency and the utter loss of privacy, accepting that secrets no longer exist. The societal impact of scandals (exposed secrets) will diminish because it is impossible to react with constant indignation when secrets are revealed all the time. Second, we will adapt to 100% privacy. Counter technologies will give us huge amounts of privacy protection, allowing us to pick our own desired level of privacy. Privacy will cost money and will be a paid service."

In 2025, 'everything will be transparent; people will not have the illusion of privacy'

Tiffany Shlain, filmmaker, host of the AOL series *The Future Starts Here*, and founder of The Webby Awards, responded, "In 2025, everything will be transparent; people will not have the illusion of privacy. This will, of course, have consequences."

About this Canvassing of Experts

The expert predictions reported here about the impact of the Internet over the next 10 years came in response to one of eight questions asked by the Pew Research Center Internet Project and Elon University's Imagining the Internet Center in an online canvassing conducted between November 25, 2013, and January 13, 2014. This is the sixth Internet study the two organizations have conducted together since 2004. For this project, we invited more than 12,000 experts and members of the interested public to share their opinions on the likely future of the Internet and 2,551 responded to at least one of the questions we asked. Some 2,511 responded to this question about the future of privacy.

The Web-based instrument was fielded to three audiences. The first was a list of targeted experts identified and accumulated by Pew Research and Elon University during the five previous rounds of this study, as well as those identified across 12 years of studying the Internet realm during its formative years. The second wave of solicitation was targeted to prominent listservs of Internet analysts, including lists titled: Association of Internet Researchers, Internet Rights and Principles, Liberation Technology, American Political Science Association, Cybertelecom, and the Communication and Information Technologies section of the American Sociological Association. The third audience was the mailing list of the Pew Research Center Internet Project, which includes those who closely follow technology trends, data, and themselves are often builders of parts of the online world. While most people who responded live in North America, people from across the world were invited to participate.

Overall, 2,511 respondents weighed in on the following questions:

> **Security, liberty, privacy online—**Will policy makers and technology innovators create a secure, popularly accepted, and trusted privacy-rights infrastructure by 2025 that allows for business innovation and monetization while also offering individuals choices for protecting their personal information in easy-to-use formats?
>
> **Please elaborate on your answer.** (Begin with your name if you are willing to have your comments attributed to you.) Describe what you think the reality will be in 2025 when it comes to the overall public perception about whether policy makers and corporations have struck the right balance between personal privacy, secure data, and compelling content and apps that emerge from consumer tracking and analytics.
>
> **Bonus question:** Consider the future of privacy in a broader social context. How will public norms about privacy be different in 2025 from the way they are now?

Since the data are based on a non-random sample, the results are not projectable to any population other than the individuals expressing their points of view in this sample. The respondents' remarks reflect their personal positions and are not the positions of their employers; the descriptions of their leadership roles help identify their background and the locus of their expertise. About 84% of respondents identified themselves as being based in North America; the others hail from all corners of the world. When asked about their "primary area of Internet interest," 19% identified themselves as research scientists; 9% said they were entrepreneurs or business leaders; 10% as authors, editors or journalists; 8% as technology developers or administrators; 8% as advocates or activist users; 7% said they were futurists or consultants; 2% as legislators, politicians or lawyers; 2% as pioneers or originators; and 33% specified their primary area of interest as "other."

On this particular question many of the respondents elected to remain anonymous. Because people's level of expertise is an important element of their participation in the conversation, anonymous respondents were given the opportunity to share a description of their Internet expertise or background.

Here are some of the key respondents in this report:

Miguel Alcaine, International Telecommunication Union area representative for Central America; **Jari Arkko**, chair of the Internet Engineering Task Force; **Francois-Dominique Armingaud**, formerly a computer engineer for IBM now teaching security; **danah boyd**, research scientist at Microsoft; **Stowe Boyd**, lead at GigaOM Research; **David Brin**, author of *The Transparent Society*; **Bob Briscoe**, chief researcher for British Telecom; **Vint Cerf**, vice president and chief Internet evangelist at Google; **David Clark**, senior scientist at MIT's Computer Science and Artificial Intelligence Laboratory; **Glenn Edens**, research scientist at PARC and IETF area chair; **Jeremy Epstein**, lead director for the US National Science Foundation's Secure and Trustworthy Cyberspace program; **Seth Finkelstein**, a programmer, consultant and EFF Pioneer of the Electronic Frontier Award winner; **Bob Frankston**, Internet pioneer and innovator; **Dan Gordon** of Valhalla Partners; **Jonathan Grudin**, principal researcher for Microsoft; **Joel Halpern** a distinguished engineer at Ericsson; **Jim Hendler**, Semantic Web scientist and professor at Rensselaer Polytechnic Institute; **Francis Heylighen**, a Belgian cyberneticist investigating the evolution of intelligent organization; **Christian Huitema**, distinguished engineer with Microsoft; **Jeff Jarvis**, director of the Tow-Knight Center at the City University of New York; **Mike Leibhold**, senior researcher at the Institute for the Future; **Herb Lin**, chief scientist for the Computer Science and Telecommunications Board at the US National Academies of Science; **Clifford Lynch**, executive director of the Coalition for Networked Information; **Alice Marwick**, author of *Celebrity, Publicity, and Branding in the Social Media*

Age; **Peter McCann**, a senior staff engineer in the telecommunications industry; **Jerry Michalski**, founder of REX, the Relationship Economy eXpedition; **Craig Newmark**, founder of Craig's List; **Ian Peter**, pioneer Internet activist and Internet rights advocate; **Raymond Plzak**, former CEO of the American Registry for Internet Numbers, now a member of the board of ICANN; **Jason Pontin**, editor in chief and publisher of MIT Technology Review; **Howard Rheingold**, pioneering Internet sociologist; **Mike Roberts**, Internet Hall of Famer and longtime leader with ICANN; **Mark Rotenberg**, president of the Electronic Privacy Information Center; **Paul Saffo**, managing director of Discern Analytics and consulting associate professor at Stanford; **Henning Schulzrinne**, Internet Hall of Fame member; **Tiffany Shlain**, founder of the Webby Awards and host of *The Future Starts Here*; **Barbara Simons**, former president of ACM and board chair for Verified Voting; **Doc Searls**, director of ProjectVRM at Harvard's Berkman Center; and **Hal Varian**, chief economist for Google.

Here is a selection of other institutions at which respondents work or have affiliations:

Yahoo; Intel; IBM; Hewlett-Packard; Nokia; Amazon; Netflix; Verizon; PayPal; BBN; Comcast; US Congress; EFF; W3C; The Web Foundation; NASA; Association of Internet Researchers; Bloomberg News; World Future Society; ACM; the Aspen Institute; GigaOm; the Markle Foundation; the Network Information Center; key offices of US and European Union governments; the Internet Engineering Task Force; the Internet Hall of Fame; ARIN; Nominet; Oxford Internet Institute; Princeton, Yale, Brown, Georgetown, Carnegie-Mellon, Duke, Purdue, Florida State and Columbia universities; the universities of Pennsylvania, California-Berkeley, Southern California, North Carolina-Chapel Hill, Kentucky, Maryland, Kansas, Texas-Austin, Illinois-Urbana-Champaign, the Georgia Institute of Technology, and Boston College.

Complete sets of credited and anonymous responses to this question, featuring many dozens of additional opinions, can be found on the Imagining the Internet site:

http://www.elon.edu/e-web/imagining/surveys/2014_survey/2025_Internet_Security_Privacy.xhtml

http://www.elon.edu/e-web/imagining/surveys/2014_survey/2025_Internet_Security_Privacy_credit.xhtml

http://www.elon.edu/e-web/imagining/surveys/2014_survey/2025_Internet_Security_Privacy_anon.xhtml

Elaborations: More Expert Responses

Following are additional provocative and thoughtful answers from other respondents, organized in the same format as those in the summary. First, the insights of those who responded “no” to the question about whether a popular and trusted privacy infrastructure would be in place by 2025. After that, there are opinions of those who answered “yes.” The report closes with additional observations that move beyond the yes/no framework.

Themes commonly found in the answers of those who say they expect there will not be a widely accepted privacy infrastructure by 2025

Theme 1) Living a public life is the new default. It is not possible to live modern life without revealing personal information to governments and corporations. Few individuals will have the energy, interest, or resources to protect themselves from ‘dataveillance’; privacy will become a ‘luxury.’

Leah Lievrouw, a professor of information studies at the University of California-Los Angeles, wrote, “A way forward for proactive, trusted privacy rights does not seem promising. Especially in the last few years, my sense is that many people, perhaps even heavy Internet users, in particular, have begun to affect an attitude of dismissive cynicism about privacy and surveillance to justify their disengagement with privacy and autonomy issues: ‘They know everything you do anyway,’ where 'they' includes anyone or anything from Google to TSA to ISP's to insurance companies, educational institutions, copyright owners, law enforcement, government, credit agencies, and so forth. I am not sure that those adopting this attitude have a very clear sense of just how extensive the data capture, and data analytics, really are, but it is a habit of mind and public opinion that does not suggest that privacy norms will be stronger in 10 years than they are now.”

Kevin Ryan, a corporate communications and marketing professional, wrote, “A secure, popularly accepted, and trusted privacy-rights infrastructure will not be possible. Business will not tolerate an Internet without analytics. Analytics will be the basis of advertising rates. Analytics is too deeply engrained in marketing. Security departments within the governments of all countries will not give up tracking activities of citizens. So long as business and the government gets the information they need, we will have ‘privacy.’ We will accept the fact that, legally and practically, we have no privacy. For most, it will not be a big deal. Clandestine networks will be created. People will create homegrown methods of avoiding scrutiny. Most people will come up with avatar aliases to do what they do not want associated to themselves.”

Joel Halpern, a distinguished engineer at Ericsson, wrote, “While the described target is highly desirable, I consider that the odds are quite high that the result of the political fighting over these issues will be significantly less than a ‘secure, popularly accepted, and trusted privacy-rights infrastructure.’ Unfortunately, I expect that we will have accepted significantly less privacy than we expect now. I hope, and expect, that we will not have given up all notions of privacy.”

Larry Gell, founder and director of the International Agency for Economic Development (IAED), responded, “By 2025, there will have been enough collection and monitoring of anyone connected to the Internet that there will be no need for privacy. Your total privacy is almost gone at this point already. The only thing needed by 2025, or earlier, is for the US government to give IBM the rights to use their new nuclear storage technology to store the masses of data and information they are collecting. They are almost there. Once you get everyone to throw away their computer and only use their cell phones for everything, you have them and everything about them. If you never knew you had any privacy rights, why would it be a problem? That is the benefit of retirement and hiring all-new, young people.”

A long-time leader of technology development for the World Wide Web responded, “Technology evolves so quickly, and thereby creates new and unique user scenarios, that it is unlikely that security/privacy infrastructures can keep pace—much less one that is generally accepted. Working in parallel with the policymakers and technology innovators will be a community whose goal is to subvert any security, liberty, and privacy advancements that are achieved.”

Peter and Trudy Johnson-Lenz, founders of the online community Awakening Technology, based in Portland, Oregon, wrote, “We expect that the hacker/geek/libertarian/individual rights community will continue to develop their own secure networks, encryption, virtual currencies, and the like within the Internet. There are also new DIY networks springing up in communities. For example, see the video ‘Free the Network: Hackers Take Back the Web’ (2012). At present, most people still assume that information about themselves is considered private unless, and until, they reveal it and make it public, although this is changing among younger people… [In reality,] information once considered private is often anything but.”

Stephen Abram, a self-employed consultant with Lighthouse Consulting, Inc., wrote, “We are in for more 'extreme' targeting, based on behavioral big data collections and matrices of all of our geo and other tagging systems as a consequence of an evolving digital economy, as well as of using the national security lever to wedge in commercial interests. There will be some 'sanctuaries' that protect privacy, but they will be few. There is actually a market opportunity for these places. Libraries will remain a bastion of private spaces, although their online access and digital content may not—vis a vis the Amazon Kindle libraries offering.”

Sam Punnett, of Fad Research, observed, “The public perception of privacy in 2025 will likely be resignation. The complexity of what constitutes a person's digital ‘fingerprint,’ and the complexity of the systems that monitor them, will remain beyond the grasp of full understanding of most individuals and policy makers. The balance will remain skewed in favour of commercial and government-associated security interests over individuals. There may be 'secure data,' but it will be secured within the opaque storage systems and protocols not readily apparent or accessible to the individual citizen. I would rule out any substantive actions by policy makers. I would not completely rule out the inventiveness of technical innovators. It is unlikely that they will craft any absolute solution that puts the individual totally in charge of his or her 'fingerprints.'"

Andrew Bridges, a partner and Internet law litigator and policy analyst at Fenwick & West LLP, wrote, "The revelations of numerous whistleblowers [like] Edward Snowden … show that governments and agencies have 'gone rogue,' having no real accountability for their actions because they have, until now, succeeded in cloaking their actions in secrecy. I fear that no amount of political pressure will bring these rogue elements under control, and there will be no trusted privacy-rights infrastructure that is effective against government surveillance. Unless government surveillance of all aspects of society and of all individuals gets under control, all norms about privacy will become hollow, and the expectation of privacy will be nil. We will have to reorder all our actions to reflect the reality that there is no privacy except for the secrecy associated with the 'Security Class,' namely those persons who get to know about others without their own actions and knowledge being known."

Barbara Simons, a highly decorated retired IBM computer scientist, former president of the ACM, and current board chair for Verified Voting, responded, "Unfortunately, I think the most likely scenario is that technically savvy people might be able to communicate privately, but most folks will not have that option. I hope I'm wrong… It would help if people would stop saying that privacy is dead—get over it. There is no law of physics that says that it is impossible to have privacy. We can have privacy, if that is what we as a society choose."

Bruce Bimber, a professor at the University of California-Santa Barbara, wrote, "At this stage, those who benefit from the market for personal information and data are well organized and have a great deal of momentum in the market. By contrast, there is little organization and few resources, comparatively, on the part of those seeking a new regulatory regime that would protect privacy. So, pressures on government at this stage are greatly imbalanced. It is impossible to make an intellectually responsible forecast for 2025, but we can certainly see that there are few prospects for comprehensive reform in the near term."

Fred Zimmerman, of Pagekicker.com wrote, "There are no market drivers to make it happen. Rather, all the market drivers are to make individual behavior as track-able as possible for consumer purposes, which inevitably means that governments can track people, too. The public will be much more accustomed to a default lack of privacy on the one hand and the need for strong cryptography or going off the grid to generate real privacy, but at a cost."

Nick Wreden, a professor of social business at University Technology Malaysia, based in Kuala Lumpur, commented, "This, for better or for worse, is a free-enterprise world, and tracking data enables companies to sell more. Just look at 'do not call' lists today, with all their loopholes. The regulation was enacted, but we are all still getting calls at dinner. The elite will have privacy safeguards, while the rest of us will not."

Karen Riggs, a professor of media arts at Ohio University, wrote, "Lawmakers (of course, being funded by corporations) might grapple with the problem in various ways, but corporate interests are overwhelmingly powerful. It is also unlikely that government officials and employees will unilaterally back off their affront to personal privacy because of what is deemed 'in the national interest.' …. A gathering storm is occurring in the realm of employer-employee relations. Among other practices, the bleeding of private Internet and communication technology (ICT usage) into the workplace is transforming the modes and scope of surveillance by employers. In less direct communication, corporate and private hacking (as well as government surveillance) will continue to creep into everyday ICT usage. Privacy protections will be Band-Aid measures. With each correction of technological vulnerability, corrupt influences find a new way to invade the personal sphere."

Ebenezer Baldwin Bowles, founder and managing editor of CornDancer.com, wrote, "Protection of personal information by the individual citizen, over-matched and out-maneuvered, is the propagandist's illusion—a hard sell come 2025. No number of outwardly friendly personal security apps will enable the individual to outsmart the profit-driven determination of major corporate players and criminal cyber gangs, or overcome the intrusions into privacy and cynical threats to liberty from a menacing fascist state, bent on total control of a restive and displaced populous. The few who retain awareness will have realized the impossibility of privacy but will learn to strike a counterbalance through the sly creation and manipulation of multiple and diverse online identities. Everyone will be watching everyone, but no one will be certain of the actual corporeal identity of the visages on the other side of screens and holographic projections. For the many, participation in the Net will no longer be optional.…There will be no escape from the chipset, the camera, and the omnipresent PDA. The long-sought passive legion of worker drones will, at last, be fully mustered and brought under systematic control by the stock-holding elite and their handsomely compensated managers, engineers, analysts, planners, and enforcers. A sophisticated menu of online social and cultural diversions, delivered in the guise of entertainment and personal networking, will satiate the wage-earning citizenry, ensuring that the so-called 'haves' remain blind to inequity among peoples and oblivious to the rapid diminishment of resources necessary to feed, house, and clothe the human race. Everyone vested in the system will have just enough to satisfy vague ideas of personal progress and opportunity...The mantra, ‘What have you got to hide?’ will have become commonplace criticism of anyone who stands against the all-powerful state in matters of privacy versus security. Not knowing our neighbors, and inculcated with deep-seated fear of ‘the other,’ we, as a people, will view privacy as one of those things we had to relinquish to be safe from harm and secure in our hovels.”

Frank Thomas, a communications professional, wrote, “The continuing influence of US corporations, the US administration, and the Chinese state with the then-largest digital user base, will inhibit effective protection of user privacy. The situation is just too good for these major players to leave individual privacy rights below the level attained with international telegraphy or postal services in the nineteenth century. Who could have imagined that private corporations demand, and get, the right to read your address book, just under the pretense to send ‘better’ advertisements (as smartphone apps often demand)? There will be a continuing struggle on privacy between countries with a historical experience of dictatorship and foreign occupation, such as the majority of European, African, Asian and Latin American countries, whose populations will demand strong privacy, and the few Anglo-Saxon countries with their Puritan and dictator-free experience, who see no evil in living digitally naked. I have nothing to hide, so the state (or a corporation) can look into my intimacy, if I get a favor for it.”

Francis Osborn, a philosopher at the University of Wales-Lampeter, wrote, "Governments and businesses are extremely unlikely to create a secure and trusted privacy-rights infrastructure because, where privacy rights and online marketisation conflict, the buying public [is] consistently ready to take a convenient option, which compromises the security of their data. There are, and will remain, a minority who wish to ensure the security of their data and privacy, ensuring the continued demand for such a secure and trusted system, but buying and selling personal data is such a large part of marketising otherwise unprofitable online services that a compromise by 2025 seems impossible.”

Dave Burstein, editor of Fast Net News, responded, “In making decisions like this, especially around monetization, corporations with the money for lobbying too often dominate. The result is weak protection for individuals. Most of us will continue to prefer our sexual behavior unobserved and will not go naked in public. Short of that, the majority will take a, ‘What the ****,’ attitude toward privacy.”

Mark Nall, a program manager for NASA, responded, “There may be the illusion of personal privacy, but there are two main drivers against true personal privacy. The first driver is corporate need to understand the customer. Business economics will continue to drive this. The second driver is national security. Lone actors are a significant threat now, and advancing technology will make them an even greater threat in 2025. Automated monitoring will be used to help prevent future crimes. There already is little or no expectation of privacy online. This will continue, so I see little change by 2025."

Celia Pearce, an associate professor of digital media at the Georgia Institute of Technology, responded, "My leaning is towards 'No,' and here is why: For one thing, policy makers are largely clueless about the Internet. They have poured billions of dollars into cyber security from the perspective of cyber-terrorism and national security, including spying on Americans, but have turned a blind eye to many other aspects of the Internet that need attention. In my opinion, the biggest threat to privacy is corporations. If we do business with them, they take our private information and can do what they will with it, pretty much entirely unregulated. They can sell our information, pass it around to their other divisions, and so on. If we browse their websites, they can cookie us and track everything we do, again, unregulated. In addition, they can spam us without consequence. At this point, corporations are free to exploit their unlimited access to our personal information without any checks or regulation, and, sad to say, I am sure this will continue… My biggest concern about the Internet at the moment is cyber-bullying and hate speech, especially misogynistic hate speech towards women. I am a video games scholar, and it is well known that, when women go into networked video games such as *Halo* or *Gears of War* speaking with their natural female voice or revealing their gender through a name or other means, they get harassed, told, 'This game is not for you,' and/or threatened with rape and so forth. And, anti-gay hate speech is so pervasive that it is commonplace. Women who speak out against sexism in the game industry are regularly threatened and harassed."

Aziz Douai, a professor of new media at the University of Ontario Institute of Technology in Canada, responded, "The high economic and political stakes involved in dominating and controlling cyberspace will continue to prevent technology innovators from creating a more secure and 'trusted privacy-rights infrastructure.' Users will be more jaded about online privacy because they will expect that it is the (huge) price they have to pay to participate in cyberspace."

David Cohn, director of news for Circa, responded, "The incentives are not aligned properly for this to occur. Publicity will be assumed; not just that it is assumed one is in 'public'—but one will assume that there could be 'publicity' around their actions. Privacy will be a privilege, and even in the act of being private, will be known. For example, I know if somebody is using Snapchat, they are having conversations that are private. Because privacy requires action, one cannot inconspicuously be private."

Tom Jennings, a respondent who chose not to share additional identifying details, wrote, "It will never happen… My guess is that the Internet as we know it—open protocols—will be replaced by inter-linked proprietary networks controlled entirely by corporate interests with a modicum of regulation and an extra heaping of government security infrastructure, a la NSA's data extraction/warehousing. Government now, and probably for another decade or two (if it is not yet already permanent), has far more pressure to serve the needs of 'business' (a misnomer: multi-national corporations, i.e., Walmart, et. al, are hardly 'business' in any historic sense). 'Apps,' as opposed to flexible multi-purpose, adaptable programs running on general purpose computers (laptops, etc.), will further ensure the death of any egalitarian use of the Net; 'apps' turn Net services and their human users into 'read-only' users consuming information produced by content-providers…[I]t is not like 'privacy' ever had a hard definition; it was always contingent upon the loss of some 'assumed' part of culture. Privacy generally meant, 'I assume no one is looking.' Corporations are exploiting components of human interaction trivia that went unexamined, i.e., tracking individual incidental purchases, or 'following you out of the store' with identity tracking, etc. Whatever happens, there will be less self-control over the consequences of our personal actions, calling that privacy, or not, is another issue."

John Anderson, director of broadcast journalism at Brooklyn College, wrote, "I just do not see that the political or economic will be there for it, unless there is a massive sea change in the way our political system works. I fear we will be living in a world where biometrics will be a common thing, and privacy will be a premium luxury commodity. This is nearly impossible to imagine, as changes in this regard are happening within generations. By and large, my students see privacy as an esoteric thing that does not really have any bearing on their lives, and that scares me."

Victor Bahl, director and research manager for Microsoft Research, wrote, "The bar for what is considered private, and for what is not, will be different from what it is today. Citizens will continue to stress about the information technology and can infer from what appears to be random and uncorrelated pieces of data. Laws will complicate the usefulness of the technology, so people will be confused about what they are giving up. Different form-factor devices will make it harder for users to understand what they are compromising."

Larry Press, a writer, consultant, blogger, and part-time professor, said, "Security and privacy will evolve, but they will not come to a stable conclusion for several reasons: first, 'right' and 'wrong' are subjective—one person's privacy for freedom fighters is another person's terrorism. Second, people willingly trade privacy for free services like those provided by Google and Facebook; that also gives those companies power to influence legislation. Third, technology—whack-a-mole—will continue to evolve. My guess is that people will be less concerned about privacy by 2025—I teach, and my students are pretty much indifferent."

Gary McGraw, the CTO for Cigital Inc., known as a father of software security, wrote, "Though all stakeholders will *want* this to happen, it will not. The government will overreach and underperform in all domains, using private industry to justify and amplify its actions. In general, the populace will remain captivated by functionality and will not care about lack of privacy, surveillance, or the tradeoffs that come as a price for ‘security.’ There will be more awareness, more worry, and about the same action by 2025.”

Karl Fogel, a partner with Open Tech Strategies, and president of QuestionCopyright.org, wrote, “I expect user privacy to be in about the same position in 2025 as it is now, for several reasons. First, businesses that provide online services often have a direct anti-privacy interest; they make their money by selling facts about their users—advertising being the most obvious use, but not the only one. Second, in online services, there is an inherent tradeoff between privacy and usability: the ‘user experience’ provided by an online service is often better the more the service knows about that user's life. (This is not to say that privacy is an unworthy goal, but rather that people sometimes want contradictory things.) Third, similarly to the above, there is a security/convenience tradeoff inherent in any software application. Software tools exist right now that offer communication free of surveillance, and in some cases, even free of detection. But, most people do not use them most of the time because those tools inevitably make communication harder for the legitimate interlocutors (after all, whenever there is a security feature that ‘does not’ involve any inconvenience, it would already be incorporated as a matter of course, thus establishing the new baseline from which the security/convenience tradeoff begins again). Fourth, governments' desire for surveillance capabilities will not go away, and neither will their strategy of drafting Internet-based services into the surveillance network…. Nothing about the passage of time changes any of these dynamics.”

Marc Weiner, a professor at Rutgers University, wrote, “The Internet's present-day commercial norms and physical infrastructure [assumes] a very elastic sense of privacy. Despite some early holdouts for a free and unregulated Internet, it was quickly monetized, and since the only things that actually move around on the Internet are data, it was data that was monetized. And, in order to monetize data, it was necessary to render conventional understandings of privacy elastic; indeed, Facebook's use of private data is the very best example of this phenomenon. This policy of elastic privacy is now so deeply embedded in the praxis of the Internet that path dependency pushes it to expand in like form.”

Theme 2) There is no way the world’s varied cultures, with their different views about privacy, will be able to come to an agreement on how to address civil liberties issues on the global Internet.

Per Ola Kristensson, a lecturer in human-computer interaction at the University of St Andrews, UK, responded, “By 2025… there will be intense pressure by the general public to legislate in order to protect people's privacy on the Internet. However, legislation will not be completed by 2025, as legislators will still be waiting for an industry-driven, privacy-rights infrastructure to be developed. The development of this infrastructure will be delayed because of an inability to agree on several fundamental issues due to competing business interests, such as a fear of standardization damaging profits for leading advertisement networks, and an inability of privacy advocates and advertisement networks and other industries profiting from profiling people to compromise. Politically, there will be serious concerns raised about how the United States risks losing its dominant position in the Internet business by legislating too harshly, as leading advertising networks by Google, Facebook, LinkedIn, and other US-based IT-companies will be even more dominant and an even bigger industry than it is today. It is likely educated people will be more reluctant to share information on the Internet, as the ability to de-anonymize people on the Internet will be much greater."

An Internet engineer and machine intelligence researcher responded, "I expect the continued balkanization of Internet governance, with different policies imposed for different reasons at the national level. Some countries will choose to favour individual privacy and information security. Others will take a laissez-faire approach. And, others will impose severe censorship and access restrictions for various well-meaning or misguided reasons. I expect established business and national security interests to continue to disrupt any attempts for global governance with regards to individual privacy and information security. It is likely that continued disclosures of privacy violations, particularly disclosures that lead to human rights violations, will raise public concerns, perhaps even to the point where citizens of democratic nations collectively express that concern by voting for government representatives who are equally concerned. It is equally likely that the public in wealthier, democratic nations will simply accept the lack of privacy, based upon the rationalization that it does not affect them personally."

Stuart Chittenden, the founder of the conversation consultancy Squishtalks, wrote, "The outcomes will revolve around the tensions between global cultures (i.e., privacy-inclined Europe, compared to the indifferent and open United States, to controlled and censored China, Russia, etc.); economic systems (i.e., free-market capitalism and quasi-socialist economies); and sociopolitical value systems (i.e., US Republican, versus Democratic, policies); as well as a simple lack of awareness and, indeed, apathy, among much of the Western world, especially the United States, when it comes to the balance between corporate messaging and the reality of Internet-based applications and tools. Public norms will be largely indifferent, with isolated groups (i.e., ACLU, consumer advocates, Snowden-esque supporters, etc.) offering cautionary, yet shrill, messages that will be ignored by the vast swathe of the media."

Shahab Khan, CEO of PLANWEL, a nonprofit organization aimed at closing the digital divide, wrote, "This issue is too diverse for all countries to agree. Superpowers always have their own interests to look after. The developing world might agree. There would be a clear divide."

Laurent Francois, executive creative strategist for RE-UP, said, “I cynically think that, in 2025, we will experience big ‘blocks’ of interfaces, probably gathered around political or cultural objectives. As there will be this sort of oligopolistic digital world, I doubt there will be a consensus between nations with very versatile geopolitical and technological strategies. There will probably be more digital worlds: we might see new, ‘off the grid’ systems, which will co-exist and live out of infrastructures initially shaped by governments. In terms of business relationships, consumers will probably value a minimum standard of privacy. But again, as it is already a very complicated mind game (just look at what we already accept when we install a Facebook app!). I am not sure that the general public will shift its attitude if the consumer experience satisfies them. I guess that it is going to become tougher.”

David Allen, an academic and advocate engaged with the development of global Internet governance, replied, “’The Internet’ is, of course, a global phenomenon. While some nations may likely produce, by 2025, such a trusted infrastructure, it seems clear that other nations most certainly will not. Europe seems likely to continue strongly on the privacy front. On the other hand, totalitarian regimes have too much at stake to follow such a dictate. Will the United States produce such an infrastructure internally? The United States moves incredibly slowly on the things. To predict, for 2025, is a chancy bet. Will some global governance structure arise to produce such a global infrastructure? That seems unlikely, particularly with the tension between the West and pointedly non-democratic states.”

Theme 3) The situation will worsen as the Internet of Things arises and people’s homes, workplaces, and the objects around them will ‘tattle’ on them. The incentives for businesses to monetize people’s data and governments to monitor behavior are extremely potent.

Anita Salem, a design research consultant, wrote, “Government and industry will both exert strong pressures to decrease our privacy. Government will continue to strengthen data mining efforts on private citizens and push for encryption keys in the name of ‘security.’ Industry will continue to put profit over ethics and create even more unusable privacy settings and will utilize our data for subtle, and not-so-subtle, purchase and market manipulations. The lack of privacy will be taken for granted. The public will not realize the power of psychometric data mining and analysis, which will be used by the privileged to shape opinion and influence laws. Public opinion will be tailored almost instantaneously based on aggregate data mining of online activity. Behavior will be more homogenized due to the ability to network cameras and computers to observe and identify aberrant behavior. New technologies and social systems will be established that are counter to this anti-privacy culture, and these hackers may exert a disruptive force.”

Dean Thrasher, founder of Infovark Inc., wrote, “The slow erosion of privacy online is a classic ‘boiling the frog’ problem. It is hard to imagine a crisis of privacy that would force regulators or lawmakers to take a strong interest in establishing and protecting privacy rights. As for technologists, there are compelling technical and financial reasons for making privacy protections as weak as possible. The technical reason is that privacy is a ‘wicked problem,’ an intersection of social norms, tacit guidelines, and accepted practices that are difficult to codify. Managing complex security and privacy rules regarding data is an expensive and error-prone task, and most companies will avoid it if at all possible. The financial reason for avoiding it is simple: Most websites and applications are funded by advertising and commercial applications that have a strong interest in knowing as much about current and potential customers as possible. In response to the weak online privacy regime, most Web participants will grow used to managing multiple profiles. They will put forward different public views of themselves in different contexts, and others will come to respect the implicit boundary lines between these profiles.”

Alf Rehn, chair of management and organization at Abo Akademi University in Finland, wrote, “Whilst I would love to think that we will be a more advanced society privacy-wise, I am a cynic when it comes to this. As privacy is becoming increasingly monetized, the incentive to truly protect it is withering away, and with so much of policy run by lobbyists, privacy will be a very expensive commodity come 2025. Sure, some of us will be able to buy it, but most will not. Privacy will be a luxury, not a right—something that the well-to-do can afford, but which most have learnt to live without.”

Christopher Wilkinson, a retired European Union official, board member for EURid.eu, and Internet Society leader, said, “This question contains contradictions which belie the ‘Yes/No’ response. I do not accept that 'compelling apps' emerge from consumer tracking and analytics. I think that these techniques have nothing to do with the user experience, but rather are designed to customise advertisers' opportunities. I would prefer to pay more for an Internet that is free of advertising. In Europe, they will not differ significantly from what they are now. The Internet operators should adapt their offerings to the privacy of individuals and to the law. With respect to apps, etc., 'privacy by design' should be the norm.”

David Ellis, course director for the Department of Communication Studies at York University in Toronto, responded, “Big corporations will always want more confidential data from customers, especially those in the targeted-ad industrial complex, since increasingly intrusive data-mining is the hallmark of success. These motives will apply less to firms whose business is not ad-supported, but instead, based on selling content and apps (and other digital retail goods). Yet, this distinction is by no means hard and fast, since lots of developers have shown they are not above deceiving end-users about their actions… By 2025, these trends are likely to be exacerbated by the appification of the Web and the growth of the Internet of Things and the far greater degree of intrusiveness they will enable.”

Andre Brock, a survey participant who shared no additional identifying details, wrote, "I foresee that the expansion of personal information collection will continue to be exploited for profit and for 'national security.' While I am tarring smartphones with a heavy brush, thanks to their proximity to our person and status as genius loci of our social spheres, I am also concerned about the number of 'quantified-self' devices (and clothing), along with the incursion of the Internet of Things in our homes (i.e., the Nest thermostat, Internet-connected refrigerators, and smart toilets)... These devices and appliances are not yet infrastructure, but given continuing trends in low-power CPU design, I am convinced that we will continue to populate our domestic spheres with information gathering devices, and I have yet to see a considerate policy protecting our information access rights.”

Brad Berens, a senior research fellow at the USC Annenberg Center for the Digital Future, wrote, “Citizen/customer/consumer/user privacy in the United States is kind of like soccer: it is the topic of a future that is never going to show up.”

Mark Andrejevic, a university professor responded, “We are embarked, irreversibly, I suspect, upon a trajectory toward a world in which those spaces, times, and spheres of activity free from data collection and monitoring will, for all practical purposes, disappear. We will continue to act as if we have what we once called ‘privacy’—but we will know, on some level, that much of what we do is recorded, captured, and retrievable, and even further, that this information will provide comprehensive clues about aspects of our live that we imagined to be somehow exempt from data collection. We are already doing this—many of us use email as if it is private, in the way that written correspondence or face-to-face conversations were private, even though we know that commercial entities, the state, and, in many contexts, employers, have comprehensive access to it. Increasingly, we will find our ability to preserve this illusion challenged, and I suspect we will adjust to these changes the way we have already adjusted to Gmail, etc. This is not to say that there will not be resistance to increasingly comprehensive monitoring, but I suspect that conceptions of privacy will be replaced by concerns over various forms of injustice and abuse, perhaps even over particular forms of entrenched power.”

Theme 4) Some communities might plan and gain some acceptance for privacy structures, but the constellation of economic and security complexities is getting bigger and harder to manage.

Sean Mead, senior director of strategy and analytics for Interbrand, wrote, “Most people will ignore, or never appreciate, how exposed they are. There will be a branded program to represent best privacy practices, but it will be deliberately ineffective. A separate network will exist for those with a commitment to privacy; the network will lack the full functionality of the Internet and only be compatible with a limited number of sites. Expectations for privacy will be narrowed, but many will still be surprised by pictures and videos among friends going viral, in situations never contemplated at the time of capture.”

An anonymous respondent replied, “For one, there will not be ‘one public,’ nor ‘one network.’ There will geo-publics with different rules (China, Napoleonic-dominated Europe Tradition, military-industrial-United States, etc.). Secondly, these geo-publics will have separate networks, and sub-partisan groups will have separate networks in those geo-publics (think darknets). Substantial portions of the world will assume they have no privacy, and in fact, will construct apps, appliances, and graphs based on that.”

Andrew Nachison, co-founder of We Media, wrote, “I needed a third choice: ‘Yes, but…’ I have no doubt that policy makers around the globe will update privacy laws. But, they will not be uniform, or uniformly applied, and they will trail commercial and non-governmental innovations. Businesses will continue to seek new and better ways to track and persuade consumers to make purchases, as well as to manage risk. Governments in democracies will remain conflicted between the interests of citizens and those of businesses that drive economies and politics; and, governments in dictatorships, so long as they survive—and like those in democracies—will depend on surveillance technologies to track and suppress dissent. I favor stronger protections for privacy. I expect tech innovators to be the primary obstacles and providers—and I do not think policy makers will lead or create the infrastructure. I suspect we will see more inconsistencies and schizophrenia—continuing erosion of expectations of privacy for communication and digital experiences—as we see today with young people who presume their digital lives and ‘vapor trails’ are public, or tracked by someone, but they do not fully appreciate what that means; and, at the same time, older people, who instinctively distrust government, fear for the safety and success of their children and worry about who has access to their data streams, especially their electronic health records.”

Nigel Cameron, president of Center for Policy on Emerging Technologies, based in Washington, DC, wrote, “This will be turbulent. A language of privacy has yet to be properly developed, which is why, so often, people seem unconcerned. No business will prosper without consumer confidence.”

A professor at Aoyama Gakuin University, in Tokyo, Japan, wrote, “It is technically impossible to create such an infrastructure because it is impossible to attach strings to data. Once you pass the data to somebody else, you just have to hope they will use it they way they told you they would. What can be done is to have stricter laws for privacy, but even that just leads companies to create longer small-print privacy statements, which nobody reads anyway. People will understand more about privacy implications of their actions on the Internet, but they will still ignore a lot of it. Also, there will be new technology that will make things more difficult to understand yet again.”

Brittany Smith, a respondent who did not share a professional background, wrote, “It will be impossible for policymakers to create a popularly accepted privacy-rights infrastructure that is trustworthy without intensive collaboration and cooperation among major corporations and public agencies such as the NSA. This will require a large cultural shift, both within these organizations and amongst the greater public. Very few citizens are aware of what is at stake in this dialogue and are not in a position to organize and advocate for their rights. I believe a trusted organization will need to emerge that can help to educate the public and work across sectors to develop a secure infrastructure. Cyber-security will be the most important issue of the upcoming decades. People will become more aware of things like passwords and their online identities. Clicking ‘Keep me logged in,’ and, ‘Remember me,’ and, ‘Save this password,’ will no longer be an option. I believe that, in the future, smartphones, wallets, and electronic devices will have built-in hardware to make them more secure, and more software solutions to create random, secure passwords that are changed frequently will become available.”

Kelly Baltzell, CEO for Beyond Indigo, wrote, “The definition of privacy is undergoing change. What we considered privacy in the past is gone. In a sense, we are moving to a more open society, where everything can be tracked and shared. This really is a full loop back to the days of the small town, in which everyone knew everyone's business. The more we rely on devices, the more tracking will become a natural outcome. Data, devices, and information are all tools. How we use these tools is the key. People have gladly given power to those who would choose to abuse it because they get captivated by the device. The devices create pleasure (studies have shown the ‘ping’ of a smart phone text hits a pleasure center), and people shrug and say, ‘Who is searching for me anyway?’ Until people choose to take back control over their thoughts and actions, online privacy will be a non-existence… Most people do not care. They are completely unaware of how much of their lives are tracked and are stunned when they find out there movements can be tracked. By 2025, this will be the norm, unless people decide to change. I hope they change, but in reality, it is looking bleak that it will happen. It is time for people to learn they have the power to make choices."

Paul M.A. Baker, associate director at the Center for 21st Century Universities (C21U) at the Georgia Institute of Technology, predicted, "There seems to be a variety of dimensions to the idea of trusted privacy-rights infrastructure. Policy makers and technology innovators do not necessarily have the same objectives, and while individuals may desire or expect secure, private information flow and transactions, there are most likely to be trade-offs that are reluctantly accepted. 'National security' will continue to be the justification for monitoring of information flows, justified by regulators, and the objective of monetizing or generating resources will drive the erosion of individual data privacy from the private sector side. I see at least two alternative scenarios: first—individuals beginning to abandon expectations of privacy, at least the way that we current expect it, and the development of workarounds such as synthetic constructed identities that will splinter the data envelope attributed to individuals—or, second—technologies that allow alternative networks of transactions (grey nets) that straddle legal and 'official' and illegal or unofficial nets."

Stacey Higginbotham, a Texas-based technology writer, and frequent blogger for GigaOM, commented, "Consumer data is so valuable in aggregate to corporations and for policy (and so cheap, from an individual perspective), that we will get paper tiger regulations that appear to protect individual data, while giving over aggregate data that is not supposed to be personally identifiable; however, that data will be easily tracked back to an individual, though we may have more protections in place that mean governments need a warrant to do so. When it comes to redlining and price gouging based on that information, I expect we will have to see some lawsuits, as opposed to laws. Congress will not go there. In terms of security, we will see some fines that will influence companies to build better security into their products from the get-go, but they will be circumvented. Right now, most companies are not thinking about that at all, so it is low-hanging fruit to start. People will be accustomed to being monitored, and it will take increasing amounts of technical savvy and paranoia to remain untracked. I believe social mores will relax on the job-finding side, so your drunken Facebook pictures or trips to strip clubs will be less harmful from an employment perspective, although possibly still something to be held over someone's head, if necessary. People will rebel if their personal spaces, such as their homes, are broadcast online, but they will ignore it if that same information is available with a warrant, or whatnot."

Ed Lyell, a college professor of business and economics, and early Internet policy consultant dating back to ARPANET, observed, "As much as one tries, it is likely to be impossible to keep ahead of hackers, independent and national state-led. The economic incentives are great, and it is technically very easy to track everything, such as Twitter having more metadata than the actual

140-character messages. My young college students seem unconcerned with maintaining their privacy, so there will be less and less political pressure to control privacy access."

An attorney working on digital issues for the US federal government responded, "I find it hard to believe that there will not, in 2025, still be a continuum of beliefs about privacy rights, from those who will trade their grandmother's social security number for a chance at a free cheeseburger, to those who will do their ever-more-difficult best to stay off the grid out of privacy concerns. Whatever the norms—and I do believe that there will be a far more robust security and privacy infrastructure in place—there will be those at both ends who object to them, and those who subvert them for political, ideological, and financial gain. By 2025—as in 2014—there will be little *reasonable* expectation of privacy. I am concerned that if that remains the legal test, there will be little legal protection of privacy. I am extremely skeptical of any possibility of a legislative solution. I am somewhat more optimistic about a technological solution. In addition, the privacy and security implications of online life are only beginning. As more and more of our lives and interaction are online, more and more data will be stored and there will be more and more ways to access, assess, and monetize it."

Themes in responses of those expecting a trusted and reliable privacy arrangement by 2025

Theme 1) Citizens and consumers will have more control thanks to new tools that give them the power to negotiate with corporations and work around governments. Individuals will be able to choose to share personal information in a tiered approach that offers varied levels of protection and access by others.

Craig Newmark, founder of Craigslist, wrote, "If capable people of good will—on both policy and tech sides—can connect, then this can happen."

Charlie Firestone, executive director of the Aspen Institute Communications and Society Program, responded, "Personal identity and privacy will likely be more secure through user-centric identification techniques. Nevertheless, it is, and will continue to be, an electronic arms race between those who will find ways of using personal information to target products and service to customers/users and those who will find ways of protecting and 'owning' personal information on behalf of the user. First, there will be greater awareness of the uses to which one's private information will be put, and second, there will be better tools to own and/or protect that information."

An Internet researcher and entrepreneur said, “I see a convergence of identifiers, where our online and offline identities, payment methods, and devices become connected (if not centralized) in ways different than our de-coupled current state. I believe the connection of these identifiers will force the creation of more stringent rules and protections regarding data protection. Within this framework, technology builders can then develop approaches that appease the many regulatory agencies. Privacy evolves slowly. We will laugh about how ridiculous Google Glass was.”

Laural Papworth, a social media educator, replied, “Policymakers will not have a role, but technology innovators now have an extremely strong customer sector that speaks back. Products that damage fidelity will be destroyed by mass word-of-mouth media before they get too far. Rights will be managed, not because of any ethical behavior, but because not to will be bad for business. Consider Google Plus making privacy such a critical part of their social network to counterpoint Facebook's perceived lack of privacy. Privacy was a short-lived, post-industrial experiment. The global village will always win against privacy. Privacy was used to divide and separate individuals from each other to weaken them. As we enter back into the village, privacy naturally disappears against convenience and the human need for connection.”

Kevin Jones, founder of Good Capital, SOCAP (social capital markets conference) and Impact Hub network, replied, “Platforms created in the sharing economy will enable average citizens to aggregate and make felt their collective power. Car sharing, room sharing, tool sharing, etc., and nonprofits that marshal people who believe in this new paradigm, will exert their power. Collective wisdom will prevail. The people will be in more control. Corporate personhood will be reined in because the corporation will be much less central in a world past peak oil as we transition to a new future. That is the future I am aiming at and designing for.”

Deborah Lupton, a research professor at the University of Canberra, Australia, commented, “Digital technology users will become increasingly aware of how their metadata and data are being used (or misused), and there will be pressure for them to be able to exert greater control over how their data are being used. There will be a greater awareness of the relationship between digital technology use, the production of personal information via this use, and the importance of knowing what happens to these data and having control over them. Consumers will be more aware of the tradeoffs between the benefits they gain from using digital technologies and the privacy issues that this use may entail. Privacy concepts may incorporate data control concepts to a greater extent than at present.”

Paul Jones, a professor at the University of North Carolina and founder of ibiblio.org, responded, “While the main part of privacy and security is peace of mind that can only be secured by strong social norms, the continuing efforts to engineer support for privacy and security will receive sustained interest and funding. In short, it will get better because we want it to get better—and we will understand what makes it better for all of us. Some of this perception of betterness may solely be the product of exhaustion and resignation, however. During the previous century of urbanization, we constantly complained of alienation and isolation. No one knew anyone quite as well as we did when we were in small towns. Now, like it or not, we are having to relearn the social behavior of small towns: how to cooperate, tolerate, or just ignore differences. Frankly, we were not so great at all of that when we were in small towns. Now, we get another chance to try to live like a Family of Mankind."

Raymond Plzak, former CEO of the American Registry for Internet Numbers, and current member of the Board of Directors of ICANN, wrote, "All of the pieces are in place today to do this. What is really lacking is the international cooperation to do so, while, at the same time, not being seen as surrendering sovereignty by, perhaps, having to modify existing practices, polices, and laws to be a part of the global system. If this is done in the right manner, so that individual rights and privacy are protected, compelling content and apps will come on their own accord. Private data, whether it be personal information, pictures, or intent that is being surrendered in the social media world today, will be shared more conservatively in the future until such time as anti-predator and anti-exploitation mechanisms can be put into place, along with rigorous enforcement meted out to violators. This will have to be done on a global cooperative scale."

Isaac Mao, chief architect of Sharism Lab, wrote, "The Snowden case gave people a strong alert that the Internet is far from secure and privacy-proof. And, China's Internet cyber attack and Great Firewall system taught all of us that the Internet is not stable, it is not personal, and it is not decentralized; however, with such strong senses, Internet users, innovators, and entrepreneurs will strive to make more new technologies to improve on that. New, disruptive architectures or tools will emerge due to the alerts Snowdens and governments give us. Privacy will be less sensitive as more technologies can be helpful to individual users, and at the same time, privacy theft will be more easy to be tracing if abuses happen."

Adrian Schofield, manager of applied research for the Johannesburg Centre for Software Engineering, wrote, "The policy makers will lag behind the technology innovators, but the demand for an acceptable, workable global network will drive the required solutions. Most people will accept that they live 'open' lives of little interest to 'snoopers' of any sort. There will be ways of securing private data."

Neil McIntosh, a British journalist working for a major US news organization, wrote, "Even in 2025, there will be a tension, because I would expect development to continue rapidly on both sides of the privacy fence, between businesses keen to acquire and monetize personal data, and a public increasingly wary of handing it over without sufficient reward. An important third party is government: recent revelations about what information it collects may have a profound impact over time on some consumers' willingness to be tracked ‘in any way’ online. But, despite this ongoing arms race, I would expect the privacy infrastructure to be built by the market because the consequences of failure are huge. We will start to hand back the digital revolution's gains in knowledge, productivity, and prosperity if this is not sorted out. Maybe privacy becomes something you pay for by 2025; sure, your phone can give you personalised recommendations on nearby restaurants right now, but if it is for free, you need to tell the world where you are and let people market products and services at you—but, if you hand over £5 a month…”

Fred Hapgood, a self-employed science and technology writer, responded, “The ability of machines to recognize and make inferences from features of everyday life, online and off, will continue to improve, and access to those abilities will get cheaper. As they do, new privacy issues will come up over and over again. By 2025, I suspect that support for imposing a much greater degree of transparency on governments and other information consumers will be much greater.”

Mark Johnson, CTO and vice president for architecture at MCNC, the nonprofit regional network operator serving North Carolina, wrote, “The IETF will incorporate encryption into default standards, greatly improving security and privacy. There will continue to be a tug-of-war between the desire for various types of ‘analytics’ and privacy concerns, though. Privacy norms have been moving, and they will probably continue to do so. People are more aware of the issues, and I expect the tools available to help individuals take control of their privacy will improve over time.”

Mike Roberts, Internet pioneer and longtime leader with ICANN and the Internet Society, responded, “This landscape is littered with ignorance and misinformation. Despite that, there will be great progress in strengthening Internet security because politicians and tech leaders are finally in agreement that it must happen. The extremes of political views on the subject will continue to be unhappy, with lack of perfection of implementation of their views. The perfect is the enemy of the good, etc. There was an interesting blog comment the other day pointing out that 18th and 19th century immigrants seldom had any personal privacy where they came from. The wide-open spaces of America allowed the creation of ‘private’ spaces for individuals, and we continue to value that. But too much of the privacy space has been consumed by silly and prudish mores related to sex. The center point of social views has, and is, moving in a more open direction. Like other social areas, there is a deconstruction/disintermediation process going on that is energized in many ways by Internet social media. The social/political space will continue to display tension between communitarian and libertarian views despite technology evolution.”

Tim Bray, an active participant in the IETF, and technology industry veteran, wrote, “I am looking primarily to the policy makers, and policies differ from nation to nation. In those nations that have a civilized respect for their citizens’ rights, there will be a policy framework that enables all network communication to be private-by-default; law enforcement access will require a fairly traditional judicial process quite unlike the blanket-blessing the NSA currently seems to operate under. I am certain there will be other nations where pervasive abusive surveillance will be the norm. I am confident that the engineers can connect the technology dots, given a solid policy foundation to work on. I hope we have a keener appreciation that privacy is a basic benefit of modern civilization, much like indoor plumbing and elections.”

Lee McKnight, a professor of entrepreneurship and innovation at Syracuse University, responded, “B2025, there will be substantial progress in developing and deploying new overlay trust, privacy, and security architectures and systems needed by business, government, and the mobile device-loving public. These can provide end-to-end privacy and security far beyond the crude patches to the wide-open Internet. As big data requires assessing lots of data dynamically, to judge patterns and make decisions, the public will, by 2025, understand that, if it buys into 'free' digital services, it is making a trade, for re-use of—anonymized and encrypted—information about themselves and their digital habits. On the other hand, government agencies—in general—will also understand the limitations on what is accepted and what is not. And then, there is the intelligence community, both in the United States and around the world, which will accept certain levels of constraint, as the cost of doing business 2025. At least publicly. So, the public will be, more or less, cool with the balance struck, which, by 2025, will be majority digital natives and well aware of the choices and trade-offs they must make every day.”

Garland McCoy, president and founder of the Technology Education Institute, said, “In those countries with ‘open gardens,’ the customer rules, and those who wish to offer up their personal information in exchange for better services—more targeted services—will have that opportunity, and for those who wish to travel the Internet in a private, secure way will be offered the ability to do so (with the understanding that the government, should they wish to, can dedicate a mainframe to cracking your key, which would cost them a good bit of time and money per individual, per packet). So, there will be choice—real choice—in the ‘open garden’ countries. In the ‘walled fortresses’ countries, well, there will be no choices. If there is a market for privacy, real privacy, then companies will provide it. You will be able to choose your level of privacy or public engagement. Obviously, as it is in the real world, those who have the money to buy real privacy and security for themselves and their family will have it, and those who do not have the money, or do not want to invest in that level of privacy or security, will have to do with what is generally offered and available.”

Dan Farber, editor with CBS Interactive, replied, “In the next decade, the various factions will move toward a more secure, popularly accepted, and trusted privacy rights infrastructure. It is in the interest of companies interacting with customers online to make them feel more secure. It will not be perfect or totally trustworthy. With software, there are too many ways for governments, corporations, and individuals to subvert privacy policies and controls for self-interest. In addition, far more personal data is coming online, which makes the problem even more difficult to manage. Unless human nature changes (which it will not), we will not be able to have full trust in whatever privacy infrastructure is developed…. As we have seen with the NSA revelation, no data is safe from those who want to access it; however, that does not mean great efforts will not be made to provide more secure privacy. Certainly, Facebook Google, Apple, Amazon, etc., will make every effort to make their customers believe they are trustworthy stewards of privacy.”

Elizabeth Albrycht, a senior lecturer in marketing and communications at the Paris School of Business, replied, “I think that the demand will be such that a certain level of privacy will be guaranteed via policy. It will not please everyone. Consumers, corporations, and governments will all have to give something up. There will be tight time frames attached to privacy as well. Privacy will be negotiated and commoditized. We will have some free guarantees (human rights-level) and then pay for various other levels. We will not assume it is like a public good (air), but it will have a measurable (quantitative) value that we have negotiated via privacy markets. None of us will be happy with the situation, but that is good. It means that control will not be in only one player's hands.”

Randy Kluver, an associate professor of communication, and global Internet researcher based at Texas A&M University, responded, “Such a framework will indeed be created. I am not sure that it will come about by policy makers, but rather, the market will demand that something be created. I do think that technology innovators will be part of this process, but I am not sure that it will, or should, be involved in some way with the regulatory process and bureaucracy. I think we all, right now, are trying to come to grips with the implications of the Snowden revelations. We will not be able to roll back the current level of surveillance, but we will come up with a new, lower standard for personal privacy and, hopefully, do a better job of policing the surveillance mechanisms.”

Giuseppe Pennisi, an employee of the Economic and Social Council of the Republic of Italy, responded, “I trust that, in 2025, there will be good balance between personal privacy, secure data, and apps. The key issue is, in my view, different: will Internet achieve a level of externalities and interdependence similar to that of previous innovations (i.e., mechanics, electricity)? It seems that, after a very innovative first 'phase,’ research now concentrates on personal returns (i.e., enjoyment), rather than on social returns through externalities and interdependence. In Europe, the trend would be towards European regulations and closer coordination among European privacy authorities."

Olivier Crepin-Leblond, managing director of Global Information Highway Ltd. in London, United Kingdom, predicted, "Despite a lot of push and pull in the lead-up to 2025, policy makers will eventually get the right balance between personal privacy, secure data, and compelling content and apps that emerge from consumer tracking and analytics. That said, there will be some periods until then, in which personal privacy will appear to have been lost forever. Only through the continuous will of privacy advocates and their supporters will governments step in to protect their citizens and regulate privacy. By 2025, blatant cases of abuse of personal privacy will have been so publicised that the public will be much better informed than it is today. People might still be intent on giving out personal information, but they will want to know why and how it will be used—and have the means to make sure companies use it as they have declared they would."

Kath Straub, of Usability.org, responded, "By 2025, biometrics will allow unique and secure identification of individuals. Apps and content will continuously tailor themselves to the needs and whims of the individual. We will interact continuously with our technology, but it will take a very different form. We will not need to hold it in our hands, for instance. The way we 'hold' and convey our identity will change, but the norms will not be that different."

Andrew Rens, chief counsel for the Shuttleworth Foundation, replied, "I answer this as 'no' for policymakers and 'yes' for technology innovators. Policymakers will likely fail in this task, unless there are changes to democratic institutions that make them more responsive to citizens and less to proxies of multinational corporations. It is not always possible to code around bad laws and policies. Lawyers and activists will likely manage to carve out policy and legal space for innovation. Then, technology innovators will create the technological basis for people to have power over their personal information. In turn, control by people over their own information and other aspects of their communication will enable the trust necessary for businesses, especially smaller businesses, to make money via the Internet. There is no shortcut to monetization; it follows from giving people power over their information. In 2025, public norms will regard privacy as extremely important. Every institution and corporation will be regarded as duty bound, morally and, in most cases, legally, to protect the privacy of people. Those who come of age around 2025 will be aghast at the lack of privacy protection in 2013. They will regard it somewhat as a current generation regards the social acceptance of smoking in the 1950s—bizarre and disgusting."

Nilofer Merchant, author of *The New How: Creating Business Solutions Through Collaborative Strategy*, wrote, "Privacy will be reformed by 2025 by new 'protocol' leaders who advocate for new freedoms. Freedom in 2025 will be understood as being able to manage your data, your privacy."

David Solomonoff, president of the New York Chapter of the Internet Society, wrote, "Internet standards groups will integrate strong end-to-end encryption into everything. Social media and Cloud services will become much more decentralized. Business models will shift so that the consumer is in control, rather than the vendor, with vendor relationship management (VRM)."

Gary Kreps, director of the Center for Health and Risk Communication at George Mason University, wrote, "I am optimistic that advances in health information technology and policy will continue to advance the security and utility of these systems for commercial and health promotion activities. I have already seen improvements in online systems that provide consumers with increased security and privacy choices for conducting their personal and professional activities. Consumer demand will help increase the sophistication of information system security in the future. As consumers become more accustomed to using information systems for a variety of commercial, entertainment, education, communication, and health promotion activities, they will become more comfortable with the security of these systems and less concerned about breaches of privacy."

Jon Lebkowsky, Web developer at Consumer's Union, responded, "I have to answer, 'Yes,' to this question; the alternative is undesirable, if not unthinkable. Innovative developers have been researching, brainstorming, and experimenting toward the right set of technical solutions since the 1990s, but creating a viable technical infrastructure will not be enough. Business adoption, smart regulation, and some degree of cultural transformation, are all required to support online privacy and security as inherent assumptions of the online agora of the future. And, the concept and urgency of privacy may change, as well. The evolving culture of sharing diminishes the cultural value of absolute privacy. In the future, we may be less guarded about our lives and less protective of at least some elements of privacy. Two important questions include: how safe and secure can we presume to be as we become less private? And, what is the minimum desirable level of privacy?"

Ian O'Byrne, an assistant professor at the University of New Haven, wrote, "I have little faith, or trust, in policy makers, governments, and businesses and their ability to secure freedom, liberty, and privacy in online spaces. I do believe in the power of the Internet, and think that programmers, coders, and those that are able to 'write' online will be able to create, protect, and secure these basic freedoms. I am beginning to think that social norms will continue to evolve and become just that—social norms. With cell phones, we initially thought it would be ridiculous to use the cell phone at dinner, out in public. Now, we are quickly getting to a point where people wear phones, cameras, and devices in public. We can use devices on flights and get online. Simply put, we are in the middle of two models. I think we will find a way. I trust human nature, for better or worse."

Marina Gorbis, executive director at the Institute for the Future, a nonprofit research organization, responded, "People will realize the value of their personal data and increasingly use it as currency in various online and offline transactions. Creation of privacy around personal data will be driven not so much by policy and regulatory changes, but instead by advances and innovations in technologies for data protection and personal data management."

Geoff Livingston, author, and president of Tenacity5 Media, wrote, "Technology companies will be forced to develop opportunities to protect personal data. We can see from Snapchat's success that people do not want every piece of information to be available for mining purposes. As the age of context progresses, the desire to remain private in some aspects of life will increase. Companies will be forced to offer this type of privacy, or they will lose customers and prospects. We will see a much more liberal view of privacy. Things we did not expect to become public will become public, and we will gladly share that information. For example, eating and exercise habits are now becoming increasingly public thanks to wearable technologies from Nike and Fitbit."

Jesse Stay, founder of Stay N' Alive Productions, wrote, "Technology will take care of this. Leaders won't have to. Peer-to-peer technologies and protocols, such as Bitcoin's blockchain, allow for better ways of letting 'users' control their own privacy, taking control out of the hands of corporations and government. We are within five years of beginning to see this happen significantly. The public will have more control over their privacy through technology that empowers the consumer over the brand."

Matthew Henry, a CIO in higher education commented, "In a little over 10 years, basic standards that run our systems of networking and commerce from basic TCP to SMTP will need to be reestablished. Just about all the bases of what we use today were established for research and 'friendly' or trusted relationships. As forward thinking as those who established these standards were, they did not see a future full of targeted abuse. Many branches of a future include pressure from policy makers to corporations. Pressure will come first from consumers and those of us who use technology on a day-to-day basis. Many compromises and innovative collaboration between corporations will need to happen. This will lead to an environment of balance of trust and release of privacy between consumer and corporations. Compromises will need to be made by all."

Theme 2) The backlash against the most egregious privacy invasions will bring a new equilibrium between consumers, governments, and businesses—and more-savvy citizens will get better at hiding things they do not want others to see.

David Vladeck, a law professor at Georgetown University, and former US Federal Trade Commission official, wrote, "The public is only now beginning to fully understand the ecosystem that underlies the Internet. As the public becomes more aware of the massive, unconsented-to collection that is taking place, it will demand greater control over person information, including tracking and the information that is entered on websites for a specific purpose. The public will not countenance, in the long-term, unconsented uses of data provided for one purpose (i.e., order fulfillment) for another, wholly unrelated purpose… At some point, Congress, or the states, one by one, will have to enact laws that provide a solid yet adaptable legal framework for privacy protection."

An anonymous respondent said, "They will have to [implement a privacy infrastructure]. There will be no other way to continue to use the Internet as widely as we do now if data cannot be protected. The loss of the Internet would bring on an economic collapse—and cause widespread loss of community. You will not only expect privacy—you will demand it."

The CEO of a technology company replied, "The free market will force policymakers and corporations to strike the right balance to protect and secure consumer data. The coming years we may see an increase in public figures being victimized by privacy violations and data leaks. In order to ensure customers continued use of digital media, both consumer rights advocates and citizens will demand increased consumer protections and businesses will lobby to protect their interests for the sake of innovation and monetization by 2025. Public norms will shift to sharing less personal content and see an increase in business and information and knowledge sharing. With companies like Snapchat, where consumers believe their communications are deleted, we may see an increase in companies that delete content shortly after it is shared as a norm in 2025 in order for the general public to share personal content and interests."

Micha Benolie, CEO and co-founder of Open Garden, wrote, "Mobile Internet will be predominant. Network infrastructures are not only built by carriers, but also by clusters of people and organizations growing their own Internet. Decentralization of the Internet will enable more privacy as well as easier and faster deployment of access to knowledge. Networks will become self-healing and self-organizing together, with organizations becoming less centralized and more horizontal."

Bill St. Arnaud, a self-employed green Internet consultant, wrote, "Companies and individuals will build a far more secure, encrypted, end-to-end Internet—i.e., a commercial TOR. There will also be much clearer requirements on opting in on any service that impinges on privacy. Companies like Google and Apple will be at the vanguard of these developments, as opposed to those companies like the telecommunications companies who have implicated in recent NSA scandals."

Doug Casey, the director of IT for a large educational organization, commented, "I sincerely believe this will be the case. Corporations are getting used to dealing with privacy and the consumerization of IT; this will be an issue that organizations and governments will need to address. I see, in the short term, a backlash of sorts in the next few years, in which individuals will become much more guarded with personal and financial information, leading to much greater control (or marketing of control—real or perceived) of private information."

Laurie Orlov, a futurist, consultant, and industry analyst, responded, "The year 2025 is only a decade away, and even as outcry about privacy invasion gets louder, more technology is being introduced that is designed to help users easily share information (i.e., Instagram) or find each other (i.e., Tinder). People are gravitating towards the sign-in-and-share, Facebook-like style of online interactions. So, as innovators deliver the tools, and as users embrace them, policymakers will continue to be way behind in both understanding tech trends—and/or part of the problem of using shared information (NSA, for example) in ways that are not anticipated. Public norms are headed towards greater acceptance of online sharing—and business innovators are racing to capitalize on that acceptance. Individuals will continue to lack understanding about the implications of participation in online environments—even as they gain understanding about one environment, technology change is always ahead of them. The longer a user agreement for use of data provided, the less likely these are to be read. See smart phone location-based apps for many examples."

Steve Jones, a distinguished professor of communications at the University of Illinois-Chicago, replied, "It is the 'while also' portion of the question that causes me to 'go negative' with my answer, followed by the phrase 'easy-to-use.' In the event that offering individuals choices for protecting their personal information can be monetized to a greater degree than using their personal information, then maybe that can happen. Otherwise, I do not think so. Frankly, I do not think they will be very different, though if nothing else, we will be still more accustomed to having less privacy (which implicitly means we will continue to have some)."

Dave Rusin, a digital serial entrepreneur, and former digital global corporate executive, wrote, "It will be a mixture of policy makers (regulators) and the free market… I envision a fundamental change of 180 degrees, whereby a user will have to grant a multi-step permission—and for marketers, your marketing will change to soliciting someone to opt-in by them granting you permission or apps separate and a part from the 'terms-of-service' provided today, written in clever legalize allowing personal information to be utilized. Moreover, unless otherwise stated, by 2025, I see individual security access and privacy laws, up there as the equivalent of HIPPA [the health information privacy law], for all those that elect to drive any commerce, free or transactional, through peering centers located in the United States and other, more advanced economies. Peering centers will serve a gateway for certification and compliance for off-shore Internet access purveyors or governments."

Christopher Castaneda, a technology developer/administrator, wrote, "[A]s more and more stories of government data monitoring are revealed, the public will more than likely begin to push back, demanding more surveillance restraint. The public will also be more critical of corporations' use of public data, especially in social media and mobile technologies. In general terms, the public will be accepting of having its data used for various legal purposes, either in a desire for more convenience, better shopping deals, or outright ignorance of what personal data is available; however, the threshold of acceptance will only go so far. In recent years, public pushback against Facebook has shown some distaste for the company's behavior. In addition, the use of mobile devices, and the data they will produce, will cause some public concern over their devices, as mobile devices are more personal than a desktop or laptop computer."

Robert Tuohy, deputy director with an organization that studies and analyzes US Homeland Security, replied, "The monetary rewards of acceptance will incentivize technologists and policymakers to find solutions that protect privacy to reasonable extent. The public will moderate its views on what it accepts with regards to privacy. It is already happening. The combination of better protections and more moderate expectations will make monetization more likely."

Jim Harper, director of information policy studies at the Cato Institute, wrote, "The challenges that exist now will still exist in 2025. Technology and social mores will still be in flux. By 2025, most people will have realized that they are in an information economy. Their behavior will be tailored to the existence of that economy, which means that they will hide some things more carefully, and they will share some things more willingly and with better, if still imperfect, awareness."

Frank Feather, a business futurist, CEO, and trend tracker based in Ontario, Canada, wrote, "Governments and other organizations have no option but to ensure security and confidentiality of personal information; however, governments have a responsibility to protect society, and thus must have the ability, according to strict guidelines, that allows them to search for and monitor criminal activity that is conducted via information systems of all kinds. I am confident that a proper balance will be struck and that court-enforced legislation will be passed."

Micheal O'Foghlu, CTO of FeedHenry, based in Ireland, wrote, "There are many developments happening. There are pressures from large players, who control much of the infrastructure. There are pressures from governments and civil rights/privacy advocates. A new compromise will be reached that shares more than before ICTs came to dominate, but it will not be as much as the privacy activists fear. In general, younger people have fewer concerns than older people. As they grow older, they will probably become more conservative but still seem more liberal than we are today. Thus, the norm will shift towards more acceptance of sharing of certain types of data, particularly if suitably anonymised."

Aaron Balick, a psychotherapist and author of *The Psychodynamics of Social Networking*, responded, "Technology develops in response to feedback from society by way of social shaping. Already, we have seen a great deal of responsive growth from a variety of online interfaces in response to the needs and desires of the populations they serve (and sometimes exploit). Social shaping is not a smooth process, and there are dominant structures that wield power more than others. That being said, I think the infrastructure with regard to security, liberty, and privacy online will continue to develop to concerns of different online cultures—individuals too will become savvier. The result will be far from perfect, but it will be responsive to changing social needs (which, themselves, are changing—i.e., relationships to privacy). There is some evidence to show that the younger generation feels differently about privacy than does the generation that precedes it. That being said, younger people do appear to be making thoughtful choices about their privacy—they may be doing differently from their parents, but it does not mean that they do not care. Public norms will shift with regard to greater tolerance and acceptance of information that may have been 'over-shared,' as there will be an entire generation who will be in the same boat on this one. New social networking platforms will continue to develop to enable different levels of privacy, and the general population will grow and learn to manage this better. Still, more information about our daily lives is uploaded into public or semi-public spaces than ever before (Google often does this on our behalf, whether we like it or not), so a certain degree of personal revelation will continue to be more available than it was in the past."

Mattia Crespi, president of Qbit Technologies LLC, responded, "I believe it is a must. It is out of question to think we can fail in getting to the right policies and find a balance by those years. Already now, the Internet of Things forces us to re-invent communications and policies, between protocols, devices, humans, and machines. By 2025, we should have reached a decent, balanced set of policies to support our interconnected lives. There will be a clear difference in the type and forms of data and privacy connected to it. For instance, I may not care if a very personal detail of mine is shared, as long it is done anonymously. I believe privacy in the future will be modular, flexible, and adaptable. There will be a strong link to time—on how long things can be kept private. Total recording will generate repositories of any action in our lives, and privacy will be more and more related to time in the sense of past actions, present actions, and future actions."

PJ Rey, a PhD candidate in sociology at the University of Maryland, wrote, "First, we need to ask what incentive structures are in place for policy makers and business executives to pursue meaningful privacy protections. Without significant reform to the electoral process and updated regulatory infrastructure, it is hard to imagine that we will see much progress. Hopefully, we will get beyond hyperbolic declarations of the 'death of privacy' and understand that privacy and publicity are often mutually reinforcing. This would allow us to have more nuanced discussions about what responsibilities we have to one another and to what standards we should hold institutions."

Gary Marchionini, professor and dean of the School of Information and Library Science at the University of North Carolina-Chapel Hill, replied, "I am an optimist. I believe that people will become more aware of the conscious and unconscious (projected exo-information) traces of their existence as they work online *and* also of the reflections of their existence added to cyberspace by other people and machines…The result will be a 2025 with strongly divergent views, beyond the political party divisions in the United States today; we could have open states (no privacy), as well as safe states (no disclosure)."

Theme 3) Living a public life is the new default. People will get used to this, adjust their norms, and accept more sharing and collection of data as a part of life—especially Millennials and the young people who follow them. Problems will persist and some will complain but most will not object or muster the energy to push back against this new reality in their lives.

A senior analyst for Internet economics and policy responded, "Business practices, and general social (as well as antisocial/criminal) behavior, has so thoroughly 'adapted' to the reality of an insecure, privacy-rights-vacating, but nevertheless popularly tolerated Internet service delivery environment that, in the absence of some near-term, catastrophe-induced 'blank-slate' overhaul of national and international laws, commercial law, and legal/regulatory enforcement mechanisms, as well as gross technical infrastructure, there is very little chance that a truly 'secure, popularly accepted, and trusted privacy rights infrastructure' will emerge by 2025. By 2025, increased public consciousness of the existential risks arising from near-universal availability of cheap technologies of (potential) mass destruction will probably have eroded expectations of privacy, to some degree. Whether such expectations will diminish faster or slower than the rate at which de jure and de facto privacy protections are lost will likely depend on the number and severity of catastrophic technology-related incidents that occur between now and then."

Jim Warren, the retired editor and publisher of several microcomputer periodicals, a technology futurist columnist, open-government advocate/activist, and founder and chair of the first Conference on Computers, Freedom, & Privacy, wrote, "It seems clear that there are too many powerful organizations—governmental, corporate, financial, etc.—who *want* to track and profile *every* aspect of every person's lives, activities, browsing interests, purchasing habits, investment efforts, personal associations, etc.—for them to *ever* 'allow' individuals anywhere nearly as much control over their own personal information, as many—most?—folks would like to have. Additionally, there is great truth in the cliché that, 'Desire for privacy is a mile wide…and an inch deep.' People want *their* privacy, but they also want to know all sorts of things about *other* people. In this case, 'people' can be as per five Supreme Court 'Justices,' and the most recent Republican Presidential candidate's twisted view—that, 'Corporations are people.'"

Jari Arkko, Internet expert for Ericsson, and chair of the Internet Engineering Task Force, wrote, "There are no absolutely private or secure solutions, nor is there absolute lack of privacy. And, there are great challenges in this area. At the same time, I am optimistic that we can and will improve the state of Internet privacy. It is clear that the society's norms are trending towards accepting more public disclosure of information related to people."

Dan Gordon, of Valhalla Partners, wrote, "Every other business infrastructure in the history of capitalism (and probably before) has started out as a 'Wild West' operation and has developed rules, frameworks, norms, balances of power, and (some) refuge or relief for the powerless. It is incomprehensible to me to think that this will not happen with the online business infrastructure. We are moving in the direction of demanding and tolerating less privacy and more shameless 'living in the limelight.' Since most of us are hungering to become celebrities with no privacy (in exchange for what—notoriety?), it is hard to see that we will value it more over time than we do today."

Herb Lin, chief scientist for the Computer Science and Telecommunications Board at the National Research Council of the US National Academies of Science, wrote, "The public is strongly conflicted about privacy. In the abstract, people want privacy, but in fact, they want privacy for themselves—but less so for other people. And, they are willing to trade off privacy for economic advantages—often very small advantages—partly because they do not realize the extent of their privacy tradeoffs and partly because they do not care enough about their privacy relative to those advantages. Moreover, they want security—and to the extent that privacy and security must be traded off, they will opt for the latter. As time goes on without a major security incident, concerns about security fade, and privacy becomes more important. But, when another security incident happens, concerns about privacy fade. The public will still be conflicted about privacy in 2025."

Robert Cannon, Internet law and policy expert, wrote, "Digital natives, as they have matured, have become savvier with their sense of privacy. They have become more astute about what they put online, and how… The norm has become kids becoming more aware that they have an online face that is visible. They may cloak their presence when they want to be less visible; they may groom their presence so that, when they are search for, there is something good to find. The fear-based message that if you tweet something bad it will be discovered persists; the real message is that we all have online presences and it is up to youth to craft what is found when it is searched for."

A technologist working in Internet policy predicted, "The sad fact is that a backdoor, or 'lawful access mechanism,' cannot be used exclusively by 'good guys' (those working in the interests of a given user) but in fact, can be equally used by 'bad guys' (those working against the interests of a given user). The engineers have already begun to harden the core Internet infrastructure, and Internet corporations are learning that they have to offer end-to-end security or they need to confine the 'monetization' of content to the ends of the communication, preferably to the client, where access has to be covert (read as: important enough to break into someone's house) or through due process. This is a fact that will lead society to prefer non-hobbled ICT infrastructure for communications. I think we will all have a better understanding of what privacy is and the value it gives us in an über-connected society by 2025. I think kids will learn about this stuff from a very early age and will continue to lead society in privacy sensitivity."

David Berkowitz, the chief marketing officer for a large advertising agency responded, "A number of models like this have been tested, and during the next 10 years or so, it is likely that one will catch on with enough support by business, corporate, and consumer interests. Relatively few individuals will actually take part in such a program though. We are already reaching a turning point of wanting to be public and private at the same time. People care more about privacy but share more publicly. Expect these extremes to continue to diverge, with far more robust privacy options and protection in 2025 than what we are used to today, but also far more shared publicly. By 2025, we will also have national and prominent local elected officials, who entered college in the early part of last decade, when social media usage started to become widespread. So, there will be a greater acceptance of people having shared things that they since regret. Granted, some of those regrets will come back to haunt such candidates and officials."

Bob Frankston, an Internet pioneer and technology innovator, whose work helped allow people to have control of the networking of the Internet within their homes, wrote, "This is a complex problem with no simple solution. The concept of privacy keeps evolving, and I hope that tolerance will improve in the face of more information being public.”

Justin Reich, a fellow at Harvard University's Berkman Center for Internet & Society, said, “The risks of privacy violations are too abstract and distal, the benefits of surrendering privacy too immediate and valued. A very small number of organizations will continue to battle on behalf of the public for stronger privacy protections, probably having some success against the most extreme transgressions, but businesses will lobby against protections under the banner of consumer choice, and harms against consumers will remain too difficult to communicate. This might be different if we have a Hoover-esque government transgression. Broadly, people do not care about Internet privacy. And, as youth who grow up in a culture of exchanging data for service get older, the public will, on average, care even less about their privacy and data security by 2025. If the Snowden revelations do not shift public opinion, what will?”

Bob Briscoe, chief researcher in networking and infrastructure for British Telecom, wrote, "Society's memory is short—Stalinism, Maoism, Nazism, and McCarthyism happened too long ago to worry about. The technology will be created, but policy-makers will not make it compulsory under pressure from corporate interests. It will not be used widely because commercial organisations have strong interests to gather information about their potential customers. Although many people are uneasy about erosion of their privacy, only a few feel strongly enough to withdraw their business from companies who put customer privacy below their desires to gather market information. Therefore the business risk of not introducing a new privacy-rights infrastructure is low for all commercial organisations. Younger people are already less concerned about their privacy than older people. I would like to think that repeated high-profile abuses of people's private information would cause a backlash, however the trend will continue towards less concern about personal privacy.”

Amy Hartman, an information science professional based in Ohio wrote, “It will evolve to continue to make money and be secure for various corporate and academic entities, as well as those individuals who understand how to manipulate code enough to protect themselves. Because of the open nature of the Web, there will always be some level of corruption, fraud, and/or spying, the same way there is in our larger society and other forums. We cannot erase basic human nature, and if there is money to be made, or power to be had by sneaking around and manipulating people and information, someone is going to find a way to do it. Most people, even now, do not really understand most of the larger privacy issues when it comes to the privacy, use, and misuse of personal information. So long as it does not impact most people's daily lives in a way they can see, I suspect norms will remain the same.”

Jeremy Epstein, a senior computer scientist at SRI International, responded, “Consumers do not care enough about their privacy to create the incentives necessary to protect privacy rights. As a result, I doubt that there will be a method for offering individual choices for protecting personal information. Consumers will continue to complain about privacy, but they will not be willing to do anything about it. We will still give up our information for a ten-cent discount on a cup of coffee or shorter lines at the tollbooth. It will be similar to the (mythical) boiling frog—we will continue to lose privacy one degree at a time, until there is none left at all.”

Chen Jiangong, an Internet business analyst in China, responded, “I think it will be. But there will be new questions. The privacy war between businesses and consumers will go on forever because the new technology will challenge the consumers’ privacy again and again. The public opinion of privacy will change; people will give up a part of secondary privacy—just as, in ancient China, women once viewed their feet as a private thing, to be kept out of public view, but now they do not. Maybe in the future, people will not view something that we think of as private today as private.”

Supten Sarbadhikari, a leader working to implement the National Health Portal of India, wrote, “Actually, the answer is not an unqualified ‘Yes.’ Shades of grey are bound to be present. While it is most likely that secure systems will be in place, and online transactions will become ubiquitous, it is also likely that potential breaches and threats to security will increase. Privacy is a relative concept. When the President of the United States gets admitted for any surgical procedure, other than the attending doctors, no one has access to the details. Whereas, when the Prime Minister of India gets admitted for a surgical procedure, a medical bulletin is broadcast every hour in the public domain. With the world becoming a smaller global village, these socio-cultural contexts may also be blurred partly.”

Peter Janca, managed services development lead at MCNC, the nonprofit regional network operator serving North Carolina, responded, “As more business transactions take place via the Internet, someone (i.e., policymakers, IETF, financial industry, or the like) will need to establish a popularly-accepted, secure method of completing such transactions. As relates to consumer tracking and analytics, I believe work will have been done by 2025 to address public perceptions on the beneficial nature of such activities. We already see the ‘younger’ generation holding a norm about privacy, which is way more open than that of the over-30 generation. This norm is more open. As this generation matures, I predict it will retain much of this openness, yielding a more open public norm about privacy. This prediction could be modified, should several (more than two or three) serious, negative, public events take place that damage the younger generation's confidence in being open (i.e., reduced level of concern about privacy).”

Daniel Castro, director of the Center for Data Innovation, wrote, "Privacy is a value that shifts over time based on culture and context. Old privacy fears will subside, and new ones will emerge as technology evolves. Consumers will accept or reject technologies based on their relative levels of privacy and the norms of the time. There is anonymity in a crowd, and as more people participate in different online forums, an individual's relative privacy will increase."

Cliff Zukin, a professor at Rutgers University, wrote, "One could argue that this is what we now have. Largely, it is secure. It is popularly accepted, and it can be broken by governments and other actors. It should be the same in 2025. The mass public will accept it as safe—but really, no information is completely 'safe,' now or then. There is a generational story here, with two full generations now living life mixing online and with direct experiences merging to a single reality. So, they will be less questioning of big data. This has always been a fact of life for them."

A survey research professional who has worked for decades for government, academic, and commercial organizations responded, "In assuming they have no privacy, people will permanently alter their credit and consumption behavior in futile attempts to 'throw off the scent' on consumer-tracking uses of their PII. Exceptions will be made for public emergency needs—pandemic flus, radiation accidents, missing persons, etc. Identity crimes will encourage the Social Security Administration to reissue social security numbers, people to permanently change their names, etc. Driver's licenses will have embedded tracking chips. Some people will stop driving. And, maybe, we will have some other weird stuff we cannot imagine now—like drone-proof venetian blinds. Well, maybe not that last thing."

Above-and-Beyond Responses: Part 2

A range of input by some respondents covered additional aspects of the issues.

‘The emotional climate around privacy and security will only increase’

Mike Liebhold, senior researcher and distinguished fellow at the Institute for the Future, wrote, “There will be many political, technological, and service efforts to improve privacy but, likely, even greater efforts by dotcoms to mine personal data, by black hat intruders to steal whatever they can, and by government’s pervasive surveillance of the entire Internet. There will undoubtedly be some very lurid tragedies as a result of mining, stealing, or surveillance, so the emotional climate around privacy and security will only increase.”

‘It is absurd to believe this is solvable at the technical infrastructure level’

Seth Finkelstein, a programmer, consultant, and EFF Pioneer of the Electronic Frontier Award winner, responded, “This is a classic case of bargaining power imbalance and asymmetric information. There is such an enormous disparity between individuals supposedly making these ‘choices’ for their information, and the businesses profiting from the monetization, that it is absurd to believe this is solvable at the technical infrastructure level. Every such proposal I have ever seen has struck me as ‘ending up’ replicating what happened with ‘license agreements’—that is, creating a take-it-or-leave-it system, where a person is essentially powerless to do anything but completely accept the corporation's terms, which are constrained only by consumer-protection law (which has been very much weakened over the years)…”

2025 debates about privacy will be more sophisticated than they are today

Jamais Cascio, a writer and futurist specializing in possible futures scenario outcomes, wrote, “I have little doubt that policy makers and technology innovators will have attempted to create a ‘secure, etc.’ information infrastructure by 2025, but I do not believe that it will yet be simultaneously secure, accepted, and trusted. We will likely see myriad smaller efforts, attempts to provide secure and acceptable service within a narrower framework (i.e., for a particular hardware vendor, within a particular community), but incompatibilities will continue to confound users, and multiple interested parties (including, but not limited to, governments and advertisers) will continue to push for exceptions and special access. I also suspect that, by 2025, we will have experienced at least one massive breach-of-trust incident, where a supposedly secure and trusted system will be broken open in an especially damaging way (i.e., Google's Gmail archives are cracked open and released). This may not set back the technical efforts, but it will severely undermine any hope for public trust in these systems. The common understanding about privacy is that it is an issue of ‘visibility’—can I, or my information, be seen by others? While that is superficially true, it is not the entirety of the issue. Privacy is about ‘control’—can I decide who gets to see my information, or is that decided for me, without my knowledge or consent? I suspect that, by 2025, the debates about privacy will be more sophisticated than they are today and will focus on this control aspect (versus the crude fear-mongering about teenagers taking selfies, etc.).”

‘Capacities of the surveillance state will always exceed protections of the people’

Jason Pontin, editor-in-chief and publisher of MIT Technology Review, responded, “The end you describe is highly utopian and combines a large number of goods, each of which would be wickedly hard to achieve. To give one example, a really ‘secure’ Internet does not exist and could not be built on the current infrastructure; we would need another Internet. On the other hand, I do anticipate significant progress on some of these goods. For instance, I think there will be renewed demands for more privacy controls from consumers and citizens, and I believe that companies and policymakers will have to satisfy those demands. On the other hand, I expect the capacities of the surveillance state to always exceed the protections of ordinary people. Perhaps, people will come to think of their private information as an asset, which they will selectively release to organizations and companies in exchange for certain conveniences or services.”

Business models are about tracking; we have not yet seen the backlash

Joe Touch, director of the Information Sciences Institute's Postel Center at the University of Southern California, replied, “Privacy is in direct opposition to the business models of the largest Internet companies. The Internet does not require a login, birthdate, or username, yet these companies continue to create ‘walled gardens’ that do—to create the information that fuels their revenue stream… The issue is not about policymakers and corporations, but rather, whether the public will continue to be comfortable exposing that information. Such norms already vary widely, and I continue to be surprised at the extent to which posts within the frame of a personal video screen, and thus to the entire world, exceed what would be posted—by the same person—to their own front door. I think we have not yet seen the backlash of the current norms of personal public exposure; we might when that generation shifts from being 'kids just posting stuff' to being in the position of establishing and protecting their company's reputation as managers.”

An ‘arms race’ between surveillance and personal protection that goes on and on

Brian Behlendorf, Internet pioneer and board member of several nonprofits and for-profits, wrote, “This struggle for the boundary of personal digital space—the digital equivalent of the boundary of my own home, in both legal and technical senses, but also the boundary of my own body and brain—i.e., the Fifth Amendment—will be an ongoing debate, unresolved and only more vigorous in 2025. We will likely give up the notion of public physical location as personal data, due to both official location tracking by governments (i.e., toll road payments, police car license plate scanning) and private-sector tools that track phone IDs, faces, and other personally-identifiable bits of data when people walk by or into retail shops or other interesting points. But, in the other direction, we will have even stronger rules and societal expectations against surveillance (government and private) upon the activities within people's homes or other enclosed spaces. There will be no tolerance for drone peeping toms, sniffing the wireless emissions from tablets, displays, and more. There will continually be new technologies for surveillance—each of which will spawn demand for counter-technologies. This arms race will become more a part of our national conversation about human rights, the concept of the confidential vote, and the rights of private individuals and companies to not be compelled to become agents of the surveillance state. I feel like I am compelled to answer, 'Yes,' because the question posits the existence of something we have today and will always have—but it does not ask any qualifying questions, such as the quality of those choices, the cost of different levels of privacy, what 'easy to use' means, etc. It also assumes that policy makers and technology innovators would work together on this, when, in reality, they may take diametrically opposed actions, as they often do today."

'There will be no privacy to speak of. We will have given it all away'

Rex Miller, a thought leader, and principal at a consultancy, responded, "The idea of nation-states will undergo major redefinition. The idea is now obsolete. They have been transcended by global commerce and global platforms like Google, Facebook, etc. These will provide secured enclaves as a value-added service. Policymakers move too slow in the current structure and cannot coordinate between different governance structures to be effective. There will be no privacy to speak of. We will have given away all of it, and there will rise groups who protect the different interests of vulnerable groups."

Many social and economic cues will depend on disclosure of private information

Jerry Michalski, founder of REX, the Relationship Economy eXpedition, wrote, "Data is easily copied anywhere. The idea that some entity is going to relent and not store our data, and that we will have confidence that our data is not replicated for nefarious use somewhere, is naive. I do not think governments and businesses, motivated as they are today to collect as much personal data as they possibly can, store it, and analyze it, will come to a reasonable understanding that works for citizens. At best, there may be a citizen revolt that sets whole new guidelines, but I am not optimistic that it will happen. By 2025, you will be considered a non-person if you do not have embarrassing photos or videos online from your misspent youth. People who were very parsimonious about sharing personal information will be less credible, and will be trusted less, because others will not be able to see any of their indiscretions—the things that make them human and more trustworthy."

‘Every person’s actions tracked and monetized continuously and pervasively’

Fred Baker, Internet pioneer, longtime leader in the IETF, and Cisco Systems Fellow, responded, “The Chinese startup Face++ is creating a technology from which it would be easy to imagine the year 2025, seeing a world similar to what is described in the movie *Minority Report*, in which every person's actions are tracked and monetized continuously and pervasively. I am hesitant to make predictions there, beyond that, if we cannot counter it, we must expect it to become reality. Per its website, ‘Face++ uses the cutting-edge technology of computer vision and data mining to provide three core vision services (Detection, Recognition, and Analysis).’ If we must assume continuous and pervasive service-based and crowd-sourced surveillance, and monetization of its results, we must also assume that the information gleaned will be available to anyone that can pay to obtain it. That essentially creates a ‘small town’ dynamic on a global scale—people become more careful about what they reveal, and everybody knows the dirty secrets anyway.”

‘Invasion of privacy will be normed by public acceptance’

Alison Alexander, a professor at the Grady College of Journalism and Mass Communication at the University of Georgia, wrote, “Privacy infrastructure will be ever evolving and never finished. Hardware and software changes will present new issues on a regular basis. Governments’ need for data will continue to raise questions for the First and Fourth Amendment. Corporations will try new ideas with intended and unintended consequences. Currently, social views on privacy vary dramatically, ranging from, ‘Nothing to hide,’ to, ‘Be careful: it lasts forever,’ to the ‘Right to be forgotten.’ … Invasion of privacy will be normed by public acceptance of what was previously considered improper. Privacy will continue to be threatened by new ways to learn more about everyone.”

The ‘other’ 1% will emerge and want to live off the grid—and that will bring scrutiny

William Schrader, the co-founder and CEO of PSINet Inc., the first commercial ISP, observed, “A small percentage of the world's population, perhaps a tiny fraction of 1% of mankind, will attempt to go off-grid or in some way disengage from big data. To accomplish this, they must own nothing that is tracked by government, such as real estate or autos, have no utilities in their name, have no bank account, and not earn a living by receiving a check or direct deposit. In short, they would only use cash, not own a phone, not have a tax identification number, etc. It is a challenging existence by today's normal standards, and it is not one that is easy to maintain without sincere discipline. I expect that these off-grid people will be treated by authorities worldwide as suspect in some way, simply because they choose not to be tracked. That alone, being off-grid, will likely be made a serious crime… The original concept of privacy is dead. The new concept of privacy is: ‘Only the government and my friends know.’"

The change in norms will even affect dinner parties and dates

Alexander B. Howard, an expert on digital issues and government, wrote, "A much higher percentage of the public will understand that any action taken in view of another human with a connected smartphone or made upon a social media platform online could end up on YouTube or the evening news nearly instantly and potentially irrevocably. The ability of politicians and other public figures to keep the public's business private will be substantially hindered, although wealthy and powerful people will continue to have the ability to pay to keep their private lives somewhat obfuscated. Social norms will evolve to a point where participants in dates and dinner parties will need to explicitly ask for agreement that conversations or other interactions be kept unrecorded."

'Transparency' will replace 'privacy' as the social norm and ideal

Marc Prensky, director of the Global Future Education Foundation and Institute, wrote, "This genie is now out of the bottle: Protection of 'private' information will become almost (or, perhaps, completely) impossible because those who want it will always be ahead of those trying to protect it. So, as the last pre-Internet generation cedes control to the new global Internet generations, attitudes toward security, privacy, and intellectual property will be very different than the way we have thought of them in the past. In many, or most, areas, transparency will replace secrecy as the norm. These changes will not happen, though, at Internet speeds but more gradually as the last pre-Internet generation slowly dies off. In the future, there will be *no* privacy of information as we as we now know it and have known it in the past—any data put online will become transparently available to all, despite any and all efforts to prevent this. 'Transparency' will replace 'privacy' as the social norm and ideal."

'Technical innovation is outpacing regulators' ability to act and react'

Glenn Edens, a director of research in networking, security, and distributed systems within the Computer Science Laboratory at PARC, a Xerox Company, wrote, "A major overhaul of the architecture of the Internet is required to meet the goals of privacy and the rampant use of personal information by commercial interests. It is not clear that these issues can be resolved by 2025 at our current pace. Technical innovation is outpacing regulators' ability to act and react. It is not clear what direction public norms about privacy will emerge. There is evidence of change, as well as a lack of interest or education about the issues. Scott McNealy once said that 'privacy is dead'—in some respects he might have been right."

A 'third option' might emerge in independent data warehouses

Bryan Padgett, research systems manager for a major US entertainment company, wrote, "The current two-sided security-versus-privacy pendulum will be replaced by a third option—perhaps independent warehouses of data controlled by independent parties, fed by data providers, and accessed by government only when necessary. With increasing amounts of data being generated for and by all users worldwide, it will continue to be used for good and bad in increasing amounts… I can see a future where it is accepted that anonymity has fallen by the wayside as the online world and the real world become even more fused; however, along with the loss of anonymity, the ability to remove and prevent others from seeing and/or using your data (or data about you) will emerge to become clearer and easier to manage from a single entity. If that comes to pass, it would only come from a government or international agreement, with academia and the private sector creating the technical solution that allows it to work."

Media literacy will be the key as technological evolution keeps changing the rules

Pamela Rutledge, PhD, and director of the Media Psychology Research Center, responded, "The privacy horse is out of the barn, in spite of the people arguing whether or not the barn door should be open or closed. A more critical issue is overcoming our anxiety over 'the way things were' and evaluating what needs to be protected for individuals, institutions, and governments. Policymakers do not have the expertise, or the incentive structure, to create adaptive regulations in an evolving environment. Technology innovators have the burden of financial accountability and will continue to balance the expansion of technology capabilities and features with the majority of consumer demands. Public perception is understandably narrow; most see privacy as being about Facebook settings or identity theft. We have unleashed a powerful tool on society without bothering to teach people how to use it. Media literacy will increasingly become the key to creating the demand for a reasonable balance of privacy and information control with commercial interests and personal experience. Our perceptions about privacy change as technology creates more things that define us and more ways to share. With technology increasingly reflecting our identity, privacy becomes equated with liberty, heightening our sensitivity to having choice. Social norms about privacy will change because increased technology adoption reduces technophobia, and technology use increases individual agency across all sectors of society. Individuals will increasingly demand to decide for themselves where, and when, the benefits of sharing outweigh the costs."

'I am not even sure if we really have a problem'

Nicholas Bowman, a professor at West Virginia University, commented, "I do not believe this will ever be a 'solved' problem, given that there is a diametric opposition between 'monetization' and 'personal informative.' A wise scholar, Steve Jones (of the University of Illinois at Chicago), once said that 'if you don't pay for content, you are the content,' and there is an enduring truth to this… At least, in 2013, the only monetary value of the Internet seems to be for nano-casted advertising, which is only possible when users tell us who they are… Unless we find a different economic model to base our information infrastructure on, there will be no solution. Frankly, I am not even sure if we really have a problem. By definition, norms are always subject to the influence of time—in the 1900s, it was inappropriate for one to show their ankles in public at a beach, yet, by the 1940s, the revealing two-piece bikini was sold to the public as a way to conserve water-proof fabrics for the war effort; in just 40 years, one's skin went from being a private affair to an expositionist one."

Two Internets— or more—might evolve

D.K. Sachdev, a consultant and adjunct professor in satellite systems, wrote, "The objectives, as stated in the question, are, technically, achievable; however, it conflicts with the business plans of major social networks that, in fact, encourage users to act against their own privacy! I believe that there is scope for two separate networks: one totally secure and the other driven by social media. In a way, that is what Blackberry created, and government users all over the world relied on it. Unfortunately, it is shrinking because of the conflicting objectives of the market place."

Thorlaug Agustsdottir, public relations manager for the Icelandic Pirate Party, replied, "There will be an alternative Web or alternative software that will offer people protection from snooping companies, while the ability to mask IP will probably still be a somewhat 'advanced knowledge,' while true anonymity will be, as it is today, just a myth (at least down to the IP level, if not to some kind of a central 'official' personal identification level). In 2025, people will be ever more concerned with online privacy."

Generational change will shift norms—a president's 'drunk selfies' won't matter

Erin Stark, a respondent who shared no additional identifying details, said, "We have been sharing so much, with so little concern, for so long; personal information is no longer owned by the individual, but by the Google's, Amazon's, and Facebook's of the world… We have grown up online… Today's concern with privacy will be non-existent by 2025; our presidents will have drunk selfies made public, and our Supreme Court justices will have tweeted and blogged their hopes and fears. This is going to result in total openness."

'The sting of revealing too much will lessen'

Pamela Wright, chief innovation officer for the US National Archives, wrote, "A new way of looking at privacy may be established. The Internet will know you—your family, your doctor, your bank, where you got coffee this morning, everything substantive and seemingly trivial about your life and what you do—and that will erase your privacy, but will also protect you. This is a frightening concept, but it is already well down the road. Norms are already changing due, in part, to the ubiquity of social media use. What my generation considered strictly private is completely shareable for the next generation… I was recently taken aback when I saw a colleague had sent out a picture on social media less than two hours after she gave birth. By 2025, this will be considered a very private way to handle the news, as everything about the birth will be available online as it is happening—from pictures to all kinds of health data. We may be more forgiving of people as we see everyone's personal foibles everywhere... In the future, I expect that no one will be able to control one's image online enough to be spotless, and the sting of revealing too much will lessen."

A 'peace architecture' is best for an 'always-on' world

Chris Uwaje, president of the Institute of Software Practitioners of Nigeria, wrote, "The stabilizing element of the future of the new, 'always-on' (AO) world will be overwhelmingly determined by a 'peace architecture' that has stubbornly eluded humanity. Therefore, today, policy makers and technology innovators may not have the ability to create a secured, popularly accepted, and trusted privacy-rights infrastructure by 2025 without first of all understanding that a global peace architecture is fundamental to the stability and survivability of the future world. Today, we assume that 'peace' is an integral part of human behavior, which, by extension, negates the philosophy of security, liberty, and privacy. Therefore, the AO world must deal with a 'peace engineering infrastructure' as the survivability tool of the future."

This is a tipping-point moment—teetering on the brink of effective 'mind control'

Mikey O'Connor, one of two elected representatives to ICANN's GNSO Council, wrote, "The public will cheerfully trade massive invasion of their personal privacy in exchange for goods and services they would otherwise have to pay for. In so doing, they will also increasingly compromise the privacy of those they interact with, albeit inadvertently. If the current privacy-awareness surge is turned back by the well-organized coalition of private and governmental surveillance lobbyists, it seems quite possible that this will be the tipping point, beyond which there is no return. Thus, by 2025, this battle will be lost—and much of our humanity with it. On the other hand, let us think positively. Global climate change may have reached that tipping point, as well—in which case, we can be spectators in a race to see which exterminates us first—humans or Mother Nature. We are at a tipping point. We are teetering on the capability of truly effective mind control. Once we have actually arrived there, the concern about privacy will simply be scrubbed off the agenda, and privacy will become ever less of a concern as the older, less plugged-in generation dies off."

'Privacy will be perceived as a part of exchange'

Polina Kolozaridi, a faculty member at the Center for New Media and Society, based in Russia, responded, "The idea of what privacy is can change noticeably in 2025. Partly, privacy will be perceived as a part of exchange. It will be more difficult to have self-image without public profile, at least when it is opened to some institutions (starting with educational and healthcare systems). Partly, there will appear new sorts of private information (like thoughts, if neuro-tech will be fast enough). The problem of 'whom I can trust here' will probably remain... It will be like Pacific Ocean of transparency and some big islands (or even continents) of abilities to hide one's personal data. It will not be easy to use such abilities... Having some profiles with information we consider private will be like owning an ID or a passport. It will be OK to trust some corporation or state to own it, but not OK to share it in some public profiles; social networking, like Facebook or Instagram, will not disclose more than now. But, there will appear chill-out, or media-out, zones when and where one may be out of all digitalization."

A distributed system of user rights will replace the current hierarchical system

One extended answer came from **Doc Searls**, director of ProjectVRM at Harvard University's Berkman Center for Internet & Society. He outlined how citizen-centered privacy protection can be created:

> "There will be a privacy rights infrastructure in place long before 2025. I believe it will materialize within the next three to five years. It will not be a top-down system, however—meaning that it will not come from big companies, or from policy makers in the United States, the European Union, or other familiar targets of today's privacy activism. Instead, it will come from new technological approaches that enable individuals and organizations to operate in full privacy without fear of surveillance. These approaches will be distributed, rather than centralized.
>
> The spread of these approaches will follow the rules of heterarchy more than those of hierarchy. Adriana Lukas defines heterarchy as 'a network of elements in which each element shares the same horizontal position of power and authority, each playing a theoretically equal role.' In fact, this is not new, nor unfamiliar. It is embodied in the Internet's founding protocols, as well as why the Internet grew so rapidly, wildly, and outside the control of companies and government.
>
> Key to our emerging privacy-creating system will be the ability of individuals to assert their own terms, policies, and preferences in dealings with others, including companies and governments—and for equal consenting parties to work out norms that do not require intervention or control by large companies or governments. The principles and practices here are also not new. They are at the heart of freedom of contract, which was abandoned by large mass-marketing and mass-manufacturing companies in the Industrial Age, when scale required 'contracts of adhesion,' such as those we 'accept' without reading. Adhesive contracts brought ease to Industrial Age hierarchical systems but are obsolete in the Internet age, when everybody brings their

own unique assets to the market's vast table, as well as growing power over what can be done with those assets.

Freedom of contract is also central to a free and open society, as well as to the architecture of the Internet's founding protocols. It is also anathema to the defaulted approaches of the phone and cable companies, by whose graces we enjoy access to the Internet. Fortunately, the Internet's system is deeper than theirs and, therefore, will prevail. Oceans outlive boats—even the biggest ones.

The end state will be one in which individuals will enjoy far more control of their personal data, and privacy in general, than they do today, and that will be good for business.

We now live in two worlds:

One is the physical world that has been around since the Big Bang, and where we have operated civilization for the last few thousand years. The norms around privacy are highly developed, and very deep, in this world. The technologies providing privacy—clothing, doors, windows, curtains, shades, shutters, and so on—are familiar and easy for everybody to understand and to use. In this world, most of us also understand and respect private spaces, even when we can see and hear into them. This is why we at least try to ignore sounds made by people sitting at the next table at a restaurant or in line at a theater. Without these small courtesies, civilization would be much less civilized.

The other is the virtual world. This world is composed of binary math—ones and zeroes—and is structured around the Internet, which puts every end at a functional distance of zero from every other end, at a cost that veers toward zero as well. This world coexists with the physical one and is very new. We can date it from the appearance of the graphical browser, the ISP, and universal email, which came together in 1995. This world is going on nineteen years old, and no norms within it approach the maturity of those in the physical world. Behavioral norms in the virtual world are provisional, immature, and far from civilized. A store on Main Street, for example, would never plant a tracking beacon in a customer's pants to report back on what the customer does after they leave the store; yet, this rude behavior is normative today on the commercial Web. By 2025, however, this kind of rudeness will be as gone in the virtual world as living naked in caves is gone in the physical world, simply

> because we will have invented the digital equivalents of clothing, doors, windows, sealed envelopes, and simple human courtesies."

New identification standards will emerge

Another extensive analysis of how a system could be created—and what the obstacles might be—came from **Francis Heylighen**, a Belgian cyberneticist investigating the evolution of intelligent organization. He wrote:

> "A key enabling technology for the future Internet will be a universal, secure standard for unambiguously establishing a person's identity. Several, albeit uncoordinated, steps have already been made in order to create such a standard, including Web-enabled electronic identification cards in several European countries, the OpenID standard, and ORCID, an attempt to ensure that publications are attributed to the right author.
>
> The reasons why standardization is slow to emerge tend to be social, economic, and political, rather than technological, as different corporations, governments and organizations are not inclined to exchange the valuable information they hold. An additional obstacle is people's legitimate fear for invasion of privacy and abuse,
>
> However, without universal regulation, abuse of private information by hackers, corporations, or governments is more, rather than less, likely, as no one knows who has access to which personal information, and as hardly any laws exist that specify what organizations can and cannot do with the information they possess.
>
> Technologically, it is perfectly possible (albeit non-trivial) to develop secure schemes that anonymize data so that only the ones that really need information about an individual can get access to the specific data they require, and to nothing else. For example, a doctor who finds you collapsed in the street should be able to consult your medical record and to send a message to your next of kin, but should not have access to your financial record. Your bank, on the other hand, should know the transactions made from your account, but not your state of health.
>
> Next to the technological challenge, the larger challenge will be to institute a system of rules and laws that specify exactly who can use which information

about a person. This system should be perfectly transparent to the individual so that you can find out exactly what happens with your data and have the right to withhold information that is not crucial to the functioning of an organization.

The general principle is that you should be able to act anonymously for any non-crucial transaction, but that the distributed intelligence system should be able to maximally extract the collective (anonymous or non-anonymous) information that will help it to make better decisions, while also being able to securely and transparently address a specific individual with personalized recommendations.

Such a regulatory standard for data protection is, at this moment, being developed by the European Union. Once such a computational and legal technology is in place, interactions across the Internet are likely to become much safer and more efficient. People are less likely to worry about the free use of public, anonymized data, such as which kinds of people are most likely to get diabetes or to buy motorcycles, but who are less willing to tolerate that commercial or government organizations would claim property or control over their personal data."