

The End of Privacy as We Know It?

By Judge Herbert B. Dixon Jr.

This article is not a science fiction prophecy. Rather, a recent Pew Research Center survey, *The Future of Privacy*,¹ caught my attention and imagination. According to the survey results, 55 percent of the responding persons believe that the concept of privacy as we know it today is rapidly disappearing. Pew sent the survey to people considered experts on technology, the Internet, or privacy. Many of the respondents have active roles as technology builders, researchers, managers, policymakers, marketers, and analysts in the Internet evolution. The responses are extremely interesting. In abbreviated and simplified fashion, the survey asked the respondents the following questions:

In 10 years, by the year 2025:

1. Will policymakers and technology innovators have created a secure, popularly accepted, and trusted infrastructure to protect privacy rights in the digital age?
2. How will the public perceive the balance policymakers and corporations have struck between personal privacy, data security, and apps that track and analyze data?
3. How will public norms about privacy be different in 2025 from the way they are now?

The responses command attention.

Although the survey was not based on any type of a scientific sampling, over 2,500 individuals responded to it.² The only broad consensus one can draw from the survey is that more than half of the respondents believe privacy interests are in jeopardy, that tracking of people's personal lives for commercial profit will increase, and that the government's access to personal information will increase. The good news, if there is any, is that *almost* half of the respondents, the remaining 45 percent, have an optimistic view that society will

protect privacy rights in the future.

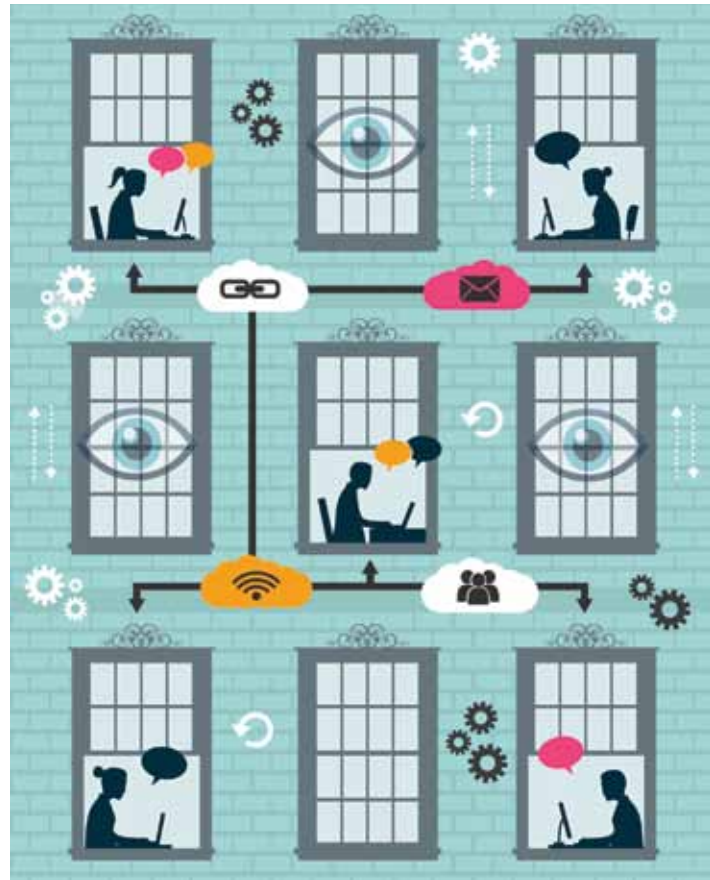
I have categorized the respondents into three groups: optimists, pragmatists, and pessimists. Individuals in the pessimist group share the belief that individual privacy, as we know this concept today, is ending. The optimist group typically gave responses with a positive view that society will protect privacy rights in the digital future. The pragmatist group, by definition, believes that people will find a way in the future to achieve an acceptable level of privacy.³

Reasons for Pessimism About Privacy in the Digital Age

The pessimist view is based on what some refer to as the boiling frog syndrome. According to this theory, a frog placed in hot water will immediately jump out because it senses the danger. However, a frog placed in cold water that is very slowly heated will not perceive the danger

and will slowly be cooked to death. This theory is a metaphor for the idea that privacy is being stripped away at such a slow pace that individuals will not recognize the danger before it is too late to do anything about it.

The pessimists concluded that privacy in the future will be diminished primarily due to (1) convenience to the consumer, (2) the need or demand for governments to provide services to and protect their citizens, and (3) the "Internet of Things" (IoT). If you have never before heard of the IoT, look around you. The IoT refers to the ever-increasing interconnection of personal and home devices through the Internet, including your ability to check the contents of your refrigerator, or its ability to check its own inventory and place orders with the grocery store to replenish supplies; check or change thermostat settings; lock and unlock doors; visually monitor rooms in the house; chart



your heart rate during the day; track the location of your children; measure the number of steps you take and stairs you climb; and locate your misplaced smartphones and other devices. In time, due to the IoT, the devices we carry and have at our homes and workplaces will tattle on us about everything we do!

The pessimist group believes that individuals will get used to the fact that mass surveillance exists and will not expect much in the way of privacy by 2025. This group also believes that government compilation of data about individuals will increase because the government has become more willing to demand data collected by commercial entities, data that the government itself cannot collect directly.

The Optimist View of Future Digital and Online Privacy

The optimists believe that individual interest and belief in privacy rights will be maintained into the future. They say that the public will become more sophisticated about security and safety and that businesses will feel pressure to implement stronger security practices such as two-factor authentication and end-to-end cryptography. This group also believes that users will insist on having the ability to encrypt their email as needed.

The optimist group believes that the future Internet will have a universal, secure standard for unambiguously establishing a person's identity. They believe that people will become more aware of the conscious and unconscious traces of their existence as they work online and that legislatures and policymakers will achieve the right balance between personal privacy and secure data.

Although the optimist group believes that egregious privacy invasions are inevitable, they also believe that a backlash will occur to bring a new equilibrium between consumers, governments, and businesses, and that the free market will force policymakers and corporations to strike the right balance to protect and secure consumer data. According to the optimists, consumer rights advocates and citizens will demand that lawmakers increase

consumer protections, and businesses will lobby the government to protect the interests of customers to continue use of digital media.

The Pragmatist View of Future Digital and Online Privacy

The pragmatists accept the notion of increased tracking of their public physical location by governments (e.g., toll road payments, police car license plate scanning) and private-sector tools that track phone IDs, faces, etc. They also believe that there will be stronger rules and societal expectations against surveillance of activities within people's homes or other enclosed spaces when, for example, people walk by or into retail shops or other commercial facilities. Pragmatists predict there will be no tolerance for drone Peeping Toms or efforts to access wireless emissions from tablets, smartphones, and other devices.

Persons in the pragmatist category believe that, to counteract the diminution of privacy that will occur due to technology advancements, individuals will create clandestine networks and other home-grown methods to avoid scrutiny and that most people will come up with avatar aliases to do things they do not want associated with their real identity. The pragmatists say that individuals will learn to strike a counterbalance through the sly creation and manipulation of multiple and diverse online identities. Although everyone will be watching everyone, no one will be certain of the actual identity of the persons on the other side of the screen or holographic projection. Today's "digital natives," as they mature, will become more deliberate in their online postings. They may even cloak their presence when they want to be less visible and groom their online presence so that, when others search for information about them, there will be something good to find.

Also, say the pragmatists, real control over private data in the future will be the privilege of those financially able to afford the cost of that control as compared with those today who can afford luxury cars, summer homes, and real privacy and security for themselves and their family.

Pragmatists say that, in the future, the customer will rule. Those who wish to offer up their personal information in exchange for better or more targeted services and convenience will have this opportunity. Those who wish to access the Internet in a private, secure way also will have the ability to do so, but with the understanding that the government, should it desire, can likely gain access to even encrypted information.

The Pessimist View of Future Digital and Online Privacy

The pessimists say that, while many folks claim to care about privacy, they care even more about convenience. Too many people will happily sacrifice their privacy for more convenience, even as they complain, including those folks who are willing to trade their grandmother's Social Security Number for a chance to get a free cheeseburger.

According to the pessimist, in 10 years, you will be considered a nonperson if you do not have embarrassing photos or videos online from your misspent youth. Individuals who are very parsimonious about sharing personal information will be less credible. They 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. The code name for this era will be "transparency"; it will replace "privacy" and "secrecy" as the social norm.

In 10 years, a small percentage of the



Judge Herbert B. Dixon Jr. is the technology columnist for *The Judges' Journal*, a member of the ABA Board of Governors, and a former chair of

the National Conference of State Trial Judges. He sits on the Superior Court of the District of Columbia and can be reached at Herbert.Dixon@dsc.gov. Follow Judge Dixon on Twitter @JhbDixon.

world's population, perhaps a tiny fraction of 1 percent of mankind, will attempt to go off-grid or in some way disengage from big data. To accomplish this, they will own nothing that is tracked by the government, such as real estate or automobiles; 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 will only use cash, not own a phone, not have a tax identification number, etc. It will be a challenging existence by today's standards, and not an existence that is easy to maintain without sincere discipline. These off-grid people will be treated by authorities worldwide as suspect in some way. Their actions will bring scrutiny simply because they choose not to be tracked. Being off-grid will be considered antisocial and a little creepy, and this conduct may even be made a crime.

Some technically savvy people will try to deploy technology to protect their privacy, but these efforts will likely be attacked or placed under intense surveillance. Folks will ask, "What have you got

to hide?" Anyone who insists upon privacy will be criticized. Privacy will be viewed as one of those things we had to relinquish to be safe from harm and secure in our homes.

The change in norms will even affect dinner parties and dates. Social norms will evolve to a point where participants in dates and dinner parties will need to explicitly ask that others not record their conversations and other interactions.

Future privacy expectations will suffer and the amount of information now available online about salaries, job descriptions, and life accomplishments will continue to increase. Even today, anyone curious about who another person is professionally or individually need only invest a few minutes in Google searches and decide for himself or herself based on the information that is retrieved. This information will likely provide a more honest portrait than what you will find on a website like LinkedIn or some other social media platform that the individual himself or herself designs.

According to some in the pessimist group, the desire for privacy can be a mile wide and an inch deep, especially in those instances where people want *their* privacy, but at the same time want to know all sorts of things about *other* people. The pessimist credits the lack of concern about privacy to complacency where individuals are willing to give up privacy for the reasons of ease, fastness, and convenience.

Although individuals talk about their desire for privacy, they increasingly use digital media and the Internet in a way that gives away their privacy voluntarily; i.e., they broadcast their location via phone GPS when posting to social platforms such as Facebook, Twitter, and LinkedIn; they photograph their entire lives with wearable devices and take selfies. For whatever reason, people are documenting their lives to the most minute detail on social media in ways that would have been unheard of to past generations. When one of the digital social media platforms reduces privacy or changes privacy settings, there is a brief uproar of public backlash; but in the end, people are not voting with their feet. They do not leave en masse. In fact, more sign up. For this reason, commercial interests

have no incentive to increase privacy, which would most likely reduce advertising, product, and service revenues. Even today, the younger generation sees privacy as an esoteric thing that does not really have any bearing on their lives.

Security organizations and departments within "the government" will insist on access to information to track individuals for security and law enforcement purposes. We will accept the fact that, legally and practically, we will have no privacy, and, for most people, it will not be a big deal.

The two main drivers against true personal privacy are the commercial need to understand the customer, which will be driven by business economics, and national security. It may be possible one day for automated monitoring to help prevent future crimes.

In the minds of some of the subject matter experts, the definition of privacy will undergo change such that what we considered privacy in the past will no longer exist, and society will become more open, where everything can be tracked and shared. Because individuals will be relying on more devices that are part of the IoT era, more tracking will become a natural outcome. Interestingly, this view draws on the analogy of life in a small town, where everyone knows everyone else's business.

Individuals will continue to complain about privacy, but they will not be willing to do anything about it. They will still give up information for conveniences such as monetary discounts on purchases, access to express lanes on the highway, and shorter lines at the tollbooth or airport. Just like the boiling frog, they will continue to lose privacy one degree at a time, until there is none left at all.

The future loss of privacy may not be all bad. One potential benefit could be improvements in face-recognition technologies. We will be able to put a name to the face of the strangers we see on the street, in the subway or supermarket, and at every sporting event. We will be able to access all the data attached to this person. A future app that will make use of this technology will alert us

In the last issue of *The Judges' Journal*, this technology column ended with the following pronouncement: As certain as anything else in life, the list of the worst passwords of 2014 will also include "password" & "123456" at the top of the list, the same as in 2013 and previous years. . . . Well, we need not wait any longer. The results are in. The people did not disappoint. The pronouncement was correct. The top two worst passwords of 2014 were the same as in 2013, namely, "password" & "123456". See <http://9to5mac.com/2015/01/20/worst-passwords>.

The biggest change among the worst passwords in 2014 is that "12345" moved up to third place from number 20 and "12345678" moved down from third to fourth. Although it is too early to predict the specific worst passwords of 2015, the results will not be much different. These same "worst passwords" will be at least in the top five this year. Count on it.

to registered sex offenders and paroled felons in our midst. When persons of the future think back on the lack of our access to this immediate type of information about the people around us, it will seem odd and unsettling, and perhaps dangerous, to think that in the past people walked, sat, and ate amid crowds of unknowable strangers.

Finally, according to the pessimists, we have embarked 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. Living a public life will become the new default. It will not be possible to live modern life without revealing personal information to governments and commercial entities. We will continue to act as if we have what we

once called privacy, but we will know that much of what we do, which we imagined to be somehow exempt from data collection, is recorded, captured, and retrievable for the world to see.

Epilogue

In which camp do you fall concerning your belief about our future digital and Internet privacy? In the words of one Pew survey respondent, today's concept of privacy will be dead in 10 years. The new concept of privacy will refer to those matters only the government and my friends need to know. ■

Endnotes

1. PEW RESEARCH CTR., *THE FUTURE OF PRIVACY* (Dec. 2014), available at <http://www.pewInternet.org/2014/12/18/future-of-privacy>.

2. Here is the breakdown of the respondents' self-classification when asked about their "primary area of Internet interest": 19 percent identified themselves as research scientists; 9 percent said they were entrepreneurs or business leaders; 10 percent identified themselves as authors, editors, or journalists; 8 percent identified themselves as technology developers or administrators; 8 percent identified themselves as advocates or activist users; 7 percent said they were futurists or consultants; 2 percent identified themselves as legislators, politicians, or lawyers; 2 percent identified themselves as pioneers or originators; and 33 percent specified their primary area of interest as "other."

3. I have not given attribution in this article for the comments that I extracted from the 2,500 individuals who responded to the survey. I have amalgamated the responses within each of the three defined groups—optimist, pragmatist, and pessimist.