



Security or Privacy: Can You Have Both?

James Bret Michael, Naval Postgraduate School

Richard Kuhn and Jeffrey Voas, IEEE Fellow

Computer hosts a virtual roundtable with six experts to discuss cybersecurity versus electronic privacy.

Since 1971, there have been more than 300 articles published in *Computer* on the topic of electronic privacy and about three times that number on cybersecurity, with many of these articles covering both topics. Roughly a third of all these articles appeared within the past five years, indicating that there is a lot of interest in security and privacy. These statistics are also telling in that *Computer* competes for content with other IEEE Computer Society publications, particularly *IEEE Security and Privacy*, which was first published in 2003.

In their seminal article from 2004, Avižienis et al.¹ treated security as one of the attributes of dependable systems, defining dependability as “the ability to deliver service that can justifiably be trusted.” They made no reference to privacy. Likewise, that same year, Voas² mentioned security but not privacy as one of the

many quality attributes of software. Looking back at these articles, one might ask, for instance, “Why wouldn’t we want both security and privacy, given our dependence on the navigation apps on our smartphones and that we need to not only trust in the integrity

of the data these apps use to compute travel routes but also in the protection of the privacy of our location data? What are the tradeoffs among security, privacy, and other system attributes, such as testability?” In a systems context, it seems natural to think about the interplay between security and privacy requirements, policies, and mechanisms.

Given the seemingly ever-growing impact of security and privacy on society, from electronic voting to computer-based contact tracing to automated driving, we thought the readers of *Computer* would benefit from a virtual roundtable in which a panel of experts provide its views on the relationship between security and privacy. To draw the attention of prospective panelists, we posed a highly charged teaser question. Is the relationship between the two terms best described as 1) security *or* privacy *or* 2) security *and* privacy; that is, can you have both? Our tactic had the intended effect. We received feedback on the title of the roundtable even before we made the questions available to the panelists. (See “Roundtable

ROUNDTABLE PANELISTS

Matt Bishop is a professor of computer science and the codirector of the Computer Security Laboratory at the University of California, Davis. He is the author of *Computer Security: Art and Science* (Addison-Wesley Professional, second edition, 2018). Bishop received his Ph.D. in computer science from Purdue University. Contact him at mabishop@ucdavis.edu.

Dorothy Denning is an emeritus distinguished professor of Defense Analysis with the Naval Postgraduate School. She has authored numerous books and articles on computer security and privacy. Denning received her Ph.D. in computer science from Purdue University. In 2019, she received the Test of Time Award from the IEEE Technical Committee on Security and Privacy. She is a fellow of the Association for Computing Machinery. Contact her at dedennin@nps.edu.

Simson Garfinkel is the senior computer scientist for confidentiality and data access at the U.S. Census Bureau. Garfinkel received his Ph.D. in computer science from the Massachusetts Institute of Technology. He holds seven U.S. patents and has published extensively on cybersecurity and digital forensics. He is a Fellow of the IEEE and the Association for Computing Machinery. Contact him at simson.l.garfinkel@census.gov.

William Stallings is an independent consultant and the author of numerous textbooks on cybersecurity, cryptography, operating systems, and computer networking. His latest book is *Information Privacy and Privacy by Design* (Pearson, 2020). Stallings received his Ph.D. in computer science from the Massachusetts Institute of Technology. He is a member of the editorial board of *Cryptologia*. Contact him at wllmst@me.com.

David Thaw is an associate research professor of law and an assistant research professor of computing and information with the University of Pittsburgh, with expertise in cybersecurity, cybercrime, cyber warfare, and privacy. Thaw received his Ph.D. from the University of California, Berkeley. He is an affiliated fellow of the Information Society Project at Yale Law School. Contact him at dbthaw@pitt.edu.

Duminda Wijesekera is a professor of computer science with George Mason University and a visiting research scientist at the National Institute of Standards and Technology. He has authored numerous articles on cybersecurity, privacy, and digital forensics. Wijesekera received a Ph.D. in mathematical logic from Cornell University and in computer science from the University of Minnesota. Contact him at dwijesek@gmu.edu.

Panelists” for more information about the panel.)

Let’s take a look at what the panelists had to say. We hope you enjoy viewing their insightful perspectives.

COMPUTER: What role does cybersecurity play in protecting data privacy? Is it reasonable to ask for security and privacy, or should it be security or privacy? To what degree can you have both?

MATT BISHOP: Whether it is reasonable to ask for both security and

privacy depends on your definitions of both “security” and “privacy.” Those definitions also underlie the degree to which you can have both. As security is defined by a security policy and these policies differ wildly among institutions and people, I don’t believe there is a simple answer to these questions. It really depends on the security policy and your definition of “privacy.”

For example, let me be precise about what “data privacy” is. To my mind, it is the ability to control who sees the data and what they can do with the data. Under this definition,

data privacy is really a variant of originator-controlled access control, with the “originator” being the subject of the data, who may not be the person generating or curating the data. Given this security policy, clearly it’s “and,” not “or.”

DOROTHY DENNING: I don’t accept the premise that security and privacy are in opposition. I don’t see how we can have data privacy without cybersecurity. Security is essential for controlling access to data. Without it, someone can steal personal data

from your devices or the computers and networks used by companies and organizations that hold your data.

In fact, cybersecurity controls, such as encryption, support privacy so well that governments want back doors installed in them so that they can get access for law enforcement and national security reasons. But installing back doors in security products weakens their security and, thus, their ability to provide privacy.

SIMSON GARFINKEL: Security is a necessary requirement for providing data privacy: without security, there is no way to prevent unauthorized access by hostile adversaries. But security is not sufficient for privacy since security mechanisms can be used to enforce policies that do not provide privacy objectives.

WILLIAM STALLINGS: There is an overlap in both objectives and technical controls. In both cases, you want to protect sensitive data from unauthorized disclosure or modification. Technologies, such as access control, authentication, federated identity, and so on, can be utilized to protect any kind of sensitive corporate data, including personally identifiable information (PII). But security controls are not enough to address privacy concerns, such as identifying uses and consumers of PII, seeking agreement to employ PII, limiting its collection and application to identified purposes, and so forth. Controls that address these privacy concerns may not be practical for security. And then you have the problem that some controls, to enhance security, can violate privacy, such as firewalls that have to do deep inspection of traffic. The tradeoff takes place at the corporate policy level, not the technical level.

DAVID THAW: Security, of course, has a role to play in implementing data privacy goals. To say otherwise would be foolish. However, the long-standing framing of the tension between “security” and “privacy” is counterproductive to discussions regarding data privacy in the digital age. Such framing is often rooted in debates regarding surveillance, such as whether or not anti-terrorism security efforts that monitor communications are run at odds with law-abiding citizens’ privacy interests in their conversations. In the purely surveillance analysis, this tension certainly exists.

Surveillance, however, is not always the issue when security and privacy interact. I would argue the contrary. In most cases where security and privacy interact, surveillance is not the issue. Thus, while it is tempting to import the surveillance framing to other contexts, this can often be misleading. Privacy is a normative choice—values-based decisions we, as a society, make regarding policies, procedures, and goals respecting the degree to which citizens can enjoy limitations on intrusion or observation of certain aspects of their lives and property. Security, by contrast, is an objective exercise; security does not have an inherent stake in how small or large the sphere of privacy is created. Once the appropriate social or political process determines the nature of privacy protections, it becomes the job of security to implement those protections within those guidelines.

Thus, when asking this question, we should at least say “security and privacy” but really are better off not framing the question this way at all. We would be better served discussing surveillance versus privacy and leaving the questions of security as

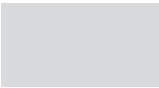
separate objective exercises in implementing whatever choices are made.

DUMINDA WIJESKERA: Yes, privacy and many forms of it are an integral and the greater part of security. I think the correct question to discuss is down in the weeds. That is, if one formalizes it, or finds a formal language to precisely specify every form of cybersecurity (even if one thinks of security and privacy as distinct entities) with respect to the same framework, then one could investigate which requirements contradict each other and which requirements can coexist. That is, there is one model of the two requirements that holds true in a single model.

COMPUTER: Are cybersecurity policy and controls the right tools for enforcing data-privacy laws, policy, terms, and conditions? If so, how do you map security policy and controls to data privacy? How do you ensure the mapping is maintained for transitive trust?

BISHOP: Whether the cybersecurity controls are the right tools to enforce the data-privacy laws, policies, terms, and conditions depends on the overlap between security and privacy. Some aspects of the data-privacy policy (which includes the relevant laws, terms, and conditions) will overlap the security policy. Others won’t. When there is overlap, the cybersecurity controls are appropriate for enforcing those parts of the data-privacy policy that do overlap.

Maintaining the mapping for transitive trust depends on your controls. Under some rare circumstances, you may be able to use cybersecurity technologies to enforce the mapping. But



for any realistic situation, you also need procedural controls, such as rights, laws, and the ability to enforce those. These will not enforce the mapping completely as one can ignore the legal and cultural norms, but to those who wish to cooperate, they can be very effective.

DENNING: Privacy policy specifies what data can be collected, who is allowed to access that information, and how the data can be used. Security policy and controls support privacy policy by protecting data from unauthorized access and ensuring that the data are adequately protected when stored or transmitted. But they cannot prevent a person who has authorized access from misusing data once acquired. Thus, some aspects of privacy policy are outside the scope of security and depend on good will, criminal prosecution, and civil lawsuits for enforcement.

GARFINKEL: Daniel Solove's "Taxonomy of Privacy"³ is a useful tool for answering this question. Solove's work identifies four primary categories of privacy harms: collection (surveillance and interrogation), information processing (aggregation, identification, insecurity, secondary use, and exclusion), information dissemination (breach of confidentiality, disclosure, exposure, increased accessibility, appropriation, and distortion), and invasion (intrusion and decisional interference). Using Solove's taxonomy, it's clear that security policy and controls are the right tools for preventing some privacy harms but not correct for others.

For example, security controls that provide for authentication, authorization, and accounting (AAA) potentially provide protection against insecurity and breach of confidenti-

ality since they allow an organization to do a better job of protecting confidential information and identify people within the organization who do not honor its commitments. At the same time, strong AAA would do nothing to stop an organization that uses inappropriately obtained information to interfere with a person's decisions.

In 2018, Mary Theofanos and I published a review article presenting "a curated list of 44 privacy historically noteworthy incidents in which individuals suffered privacy harms that were not the result of data breaches."⁴ Of these, 21 took place under the purview of the organization, but 23 resulted from software bugs, the action of an individual or a few people, or a small group acting within the organization. Better accounting combined with internal audits within an organization could have stopped many of the privacy incidents in the second category, while external audits would have been needed to prevent or minimize the 21 privacy incidents in the first category.

STALLINGS: The National Institute of Standards and Technology (NIST) has been a leader in this area. In January 2020, NIST issued its Privacy Framework, which is a companion to the NIST Cybersecurity Framework, and this framework provides guidance on using security and privacy controls for privacy risk management. It is a management-oriented policy and planning tool. To back that up are NIST special publications SP 800-53 and SP 53 A, which list a huge number of controls, with commentary and evaluation guidance plus an indication of which ones support security, privacy, and or both. So these are tremendously

important tools for security and privacy managers.

THAW: Bluntly, yes. Much of my answer stems from the reasoning behind my discussion of the first question regarding the framing of security versus privacy—that is the wrong framing. Security is a tool that implements goals privacy lays out.

WIJESEKERA: I think that this question presupposes that the terms security policies and controls refer to access control or flow control policies. If one expands the definition of "controls," then privacy controls would be within the context of the same framework that can expect to answer the question in more specific contexts as referred to in my answer to the first question.

COMPUTER: What currently prevents society from preventing or effectively pushing back against flagrant disregard of data privacy by companies that collect or infer information about individuals?

BISHOP: I think a lack of will, resources, political clout, or some combination of these. Lawsuits are expensive, time-consuming, and draining to the victims, and indeed, they may not even be possible (for example, what is a "flagrant disregard of data privacy" in one country is perfectly acceptable in another). Legal or political action requires that the lawmakers or politicians want to and are able to help. This usually involves some sort of organized campaign to bring the problems to their attention and make clear the need to (and benefits of) dealing with the problems. Remember President Franklin Delano Roosevelt's famous dictum:

“Okay, you’ve convinced me. Now bring pressure on me!”

DENNING: It is impossible to prevent any company from scouring the Internet for images or other types of data that are publicly accessible and then using those data to create a product or service, such as facial recognition software. However, if the company disregards privacy, there will be pushback, including bad publicity and lawsuits. For such pushback to be effective, we need strong privacy laws about data collection and use so that there is a legal basis for the lawsuits and criminal prosecution for violations.

STALLINGS: Sad to say, I think that is a lost battle. There used to be a clear consensus against mass surveillance and other privacy-invasive practices. In the United States, there was a willingness to take a big step back from that for many people after the terrorist attacks that occurred on September 11, 2001. Many seemed to believe the tradeoff a valid one. The government could monitor email and phone traffic in exchange for keeping us safe. Similar thinking occurred in other countries. But the pandemic spread of COVID-19 has dramatically eroded what resistance remained. We see a lot of demonstrations, but by and large, my sense is that people will accept all that goes along with contact tracing in exchange for safety from the virus. I doubt we will go back from that after the virus is brought under control.

THAW: I think the answer is that the question is wrong. It assumes that society is not pushing back. At best, we don’t yet know whether, and if so how effectively, society has been able

to “push back” against certain types of surveillance. The results of such pushback would not be truly determinable by the markets for months (if not years), and legislative policy responses can take even longer.

Instead, I would suggest that we need to analyze both market and political responses to a range of surveillance capitalism technologies over time and use those analyses to determine whether effective economic or political mechanisms exist to represent the interests of all members of society. In short—the jury’s still out.

WIJESSEKERA: I need to know more about the details prior to commenting on this question. This issue relies not only on the technical capabilities but also on what has been legislated as privacy laws, crimes, and so forth as well as how courts have interpreted them, such as narrow majorities in appellate courts carving out a special interpretation of the laws to suit their political paybacks. Both bringing the flagrant violations to notice and taking actions require a substantial effort that is not always there as long as one segment of the community profits sufficiently to prevent them from feeling violated; that is, there is a financial disincentive to advocate for laws, preventive mechanisms, and enforcement. Conversely, some of the legislative definitions that articulate the constraints preventing privacy violations may not be 100% in sync with the technical capabilities that can be expected of products and the willingness to enforce the breaches.

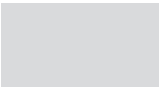
COMPUTER: What does it mean to strike a balance between security and privacy concerns, given that users clamor for anonymity and the

protection of their PII but then exhibit risky online behavior by using digital services that are well known or suspected to be collecting information about users and that do not have good track records of protecting the confidentiality, integrity, and availability of PII?

BISHOP: I’m not sure you can balance privacy and security when users behave in ways that endanger privacy or security. First, ideas of what information about people is “private” differs among individuals, so what one person might deem “risky,” another might think is perfectly safe. Second, and more importantly, people might not realize what online behavior creates a risk to their privacy. Most websites will state what information they collect and how it will be used, but this is rarely a simple and straightforward exposition. The statements usually read like the “terms of use” for programs, so they can be very long and are couched in legalese, which is hard for most people to understand. Also, to whom are the sites collecting such information “well known or suspected” and have a poor track record? Those of us in cybersecurity can usually find this information, but the average noncybersecurity user probably can’t.

DENNING: What is there to balance? I’m concerned about both. Perhaps many users are uninformed or ambivalent about both security and privacy. They might deem their behavior consistent with the perceived risks.

GARFINKEL: There has been more than two decades of research on this topic, which is broadly called “the privacy paradox.” Some research has shown that users exhibiting risky online behavior



are sometimes not aware of the risk, but at other times, they simply assess the risks and benefits differently than privacy “experts.” Other research has found that many users engage in risky behavior either because they believe that they are in fact adequately protected or because they believe that their data are already compromised and have nothing more to lose. We also know many users attempt to protect themselves through compartmentalization or by providing inaccurate or incomplete information, but these defenses are significantly harder to quantify. (This would be like giving respondents a survey asking how often they lie on surveys.)

STALLINGS: I don’t think this is an issue of a balance between security and privacy. This is a pure privacy risk issue. The majority of people don’t focus on this issue, and, frankly, I don’t think they are that much interested in it. Curbing unnecessary privacy risks and violations falls to activists, groups like the Electronic Frontier Foundation, and government lawmakers and regulators.

THAW: I also disagree with the framing of this question. What we’re really talking about here is striking a balance between surveillance concerns and privacy concerns. And there’s decades of good literature discussing why this is hard for consumers. Much of it centers on whether users actually have an effective market-participant “choice.” If all your friends and family are on a given social network, do you really have a meaningful choice not to use that network? If all the local media in your region (and all the national media in your nation) use various surveillance technologies for their websites, apps, and so forth, do you really have a meaningful choice? These questions

can richly be debated, but these are the types of questions we should be asking about the balance between surveillance and privacy.

WIJESEKERA: You cannot have it both ways. The second issue is that the definition of PII expands with technical advances, but the legislated definition changes slowly. Thus, one may take advantages of this varying gap.

COMPUTER: Many people around the globe have been the victims of data breaches. At what point does privacy, or for that matter security, matter to them since their PII is already circulating in the wild?

BISHOP: Data breaches do not result in the compromise of the same type of information for all breaches. One may reveal my financial state; another, a medical condition; and a third, information that does not compromise my privacy until it is combined with data from a fourth breach. So protecting privacy, even after a data breach, is important; the same is true of security. After all, if an attacker breaks into a company’s computer system and reads confidential data, the company does not (or should not) say, “well, it’s out there, so we don’t need to protect anything anymore.” By analogy, the same goes for privacy breaches.

DENNING: Even if the data held by one of your service providers are exposed in a data breach against that provider, there is likely considerably more information about you held by other providers. The security of that data will still matter to you.

In addition, many of the PII data that are exposed in a breach become

obsolete. For example, stolen credit card data have short lifetimes since card owners get new numbers when the breach is discovered. Similarly, a stolen password is useless once the owner knows about the breach and changes it. I don’t know of anyone who gives up on security or privacy after these breaches. More likely responses include using stronger passwords, adopting two-factor authentication, and freezing credit accounts.

GARFINKEL: The obligation of a data custodian to ensure that the security and privacy of data continues even if the data subjects have been the victim of data breaches. This makes sense from a practical point of view because there may be new potential attackers who do not have access to the data that have been compromised. It makes sense from a legal point of view: an organization’s legal obligation to protect data doesn’t stop if other organizations have been careless. Finally, there is a moral requirement, stemming from the fact that privacy is a human right, as established by Article 12 of the 1948 Universal Declaration of Human Rights.⁵

STALLINGS: It has reached a point, I think, where the members of the public tunes all the talk about privacy out unless they have a specific experience, such as a credit card theft. There are so many data being collected, many of them PII related, that the average person just can’t wrap his or her arms around the privacy issue. And I think 5G takes us beyond the ability to hope to have firm control of privacy practices. With 5G, data can be transmitted from billions of Internet of Things (IoT) devices to and through mobile carriers to a variety of consumers. The data are

much more specific and in greater volume by orders of magnitude from what has gone before. Regulations, such as the European Union's General Data Protection Regulation 2016/679 (GDPR), may help somewhat in requiring organizations to be transparent with how the data will be stored, processed, and disseminated and how they can obtain consent related to individuals' PII, but I think the implications of 5G and IoT are too broad for regulations to keep pace.

THAW: PII is a potential red herring. So-called PII is only a security threat vector if other parties require its use for authentication purposes, as opposed to identification purposes. This is a distinction I'm concerned has received far too little attention the past two decades. We should care greatly, for example, if ATM PIN codes are compromised in a breach. That is a security risk. But we should not have a system where the account number is similarly vulnerable—yet this is exactly what happens with credit cards (at least in the United States). Because, for many intents and purposes, the credit card number is both the identification and the authentication credential, it is very difficult to create secure and usable systems. A similar problem exists for Social Security numbers.

The real questions we need to be asking are about how we can redesign systems to prohibit the dual usage of information as both identification and authentication credentials. Your username never should be your password.

WIJESEKERA: It will not matter—it's only a matter of how much time or effort one wants to spend on obtaining information about any individual.

COMPUTER: Numerous security vulnerabilities have been identified in electronic conferencing and chat applications, in some cases resulting in user data being misappropriated by unauthorized third parties. Can such vulnerabilities be dealt with effectively, or should users just lower their expectations for data privacy, data security, or both?

BISHOP: Some vulnerabilities can be dealt with effectively; others can't. If it's a technical issue, then it can and should be dealt with quickly; for example, if the session is enciphered using a weak cipher, that can and should be changed. But if it's a nontechnical issue, then resolving it may be very difficult. To continue the example, in some countries, it might be illegal for information encrypted using a strong cipher to transit any part of the country without the key being registered with the government. The way to deal with this (figure out which countries to avoid? keep the weak cipher? automatically register the key? remind the user to do so?) may not be clear, and once a solution is proposed, examining it for effectiveness and compliance is another problem.

Whether users need to lower their expectations depends on what those expectations are. Having the most secure conferencing and chat applications won't help if an attacker has compromised one of the endpoints. A good rule of thumb is not to say or send anything that you would not want made public. Like any rule of thumb, it has exceptions (you may have no choices; for example, you may need to have a remote medical consultation).

DENNING: In some cases, users can adopt practices that help protect against

this, such as using end-to-end encryption and requiring passwords to enter a conference or confirmation from the host. And vendors usually fix vulnerabilities after they are discovered and reported. But it's wise to assume that new vulnerabilities will always be found and take that into account when sharing information online.

GARFINKEL: Numerous security vulnerabilities have been identified in all kinds of software, including operating systems, word processors, the telephone system, smartphones, and so on. Security vulnerabilities must be addressed, and they won't be tackled if users lower their requirements for privacy or security.

With specific reference to electronic conferencing and chat applications, many of these applications were developed without clearly articulated security models by organizations that may not have prioritized security and privacy. Fortunately, these systems can be improved. In the meantime, there is a free market, and organizations that prioritize security will presumably exercise their market power.

STALLINGS: Of course, they can be dealt with effectively. There are explicit requirements in regulations like the GDPR and similar regulations in other countries. There are a number of documents that represent wide consensus on best practices, including the NIST documents I mentioned earlier, the International Standards Organization's ISO 29000 series of privacy standards, and the privacy aspects of ISACA's Control Objectives for Information Technologies and the Information Security Forum's Standard of Good Practice for Information Security 2018. Industry-specific guidance includes

the Payment Card Industry Data Security Standard. And increasingly, corporate privacy officers are well qualified to manage the implementation of privacy controls. Even so, with all the costs involved in doing effective privacy by design, it will take public interest and strong regulatory enforcement to maintain good privacy practices.

THAW: Bluntly, yes. This is not a “hard” problem. Sure, there are some edge cases that are interesting, and assuredly, more such edge cases will develop as newer apps with differing designs are created. I expressly do not address the issue of government-authorized surveillance here as that is a separate question that needs to be answered separately.

WIJESEKERA: Both, as the search for vulnerabilities and their discovery during reverse engineering, red-teaming, and forensics investigations continue, and should. The best efforts there would make it costly for attackers, but the user community has to be aware of the exact nature of security guarantees—that they are limited in scope, apply only to one kind of vulnerability exploitation in one context, and do not provide a global, blanket coverage or liability of breach.

COMPUTER: Recent laws and regulations, such as GDPR and the California Consumer Privacy Act of 2018 (CCPA), which went into effect 1 January 2020, were designed to enhance privacy protections. Are they having an effect on privacy and security practices? What about compliance issues, given the lack of global, and in some cases, domestic harmonization (for example, between states within the United States) of privacy laws and regulations?

BISHOP: I believe they are having an effect on privacy and security practices. Many non-European institutions that collaborate internationally, or have international branches, are moving to comply with the GDPR. The same is true for institutions falling under the CCPA. I have heard of some institutions (notably web servers) blocking European connections to avoid having to deal with GDPR. That’s an effect, although not a desirable one.

Compliance issues become very interesting when the rules for which compliance is required contradict one another. At that point, you need to get a lawyer involved so he or she can advise you.

DENNING: Laws and regulations are having a positive effect. As a California resident, I’ve seen more attention to privacy from service providers that hold confidential information.

A greater harmonization of privacy laws and regulations would also help. The California law and other state privacy laws would be good starting points for federal legislation.

GARFINKEL: For me, the main impact of GDPR is that I must now click to “accept cookies” for nearly every non-U.S. government website that I visit. For the CCPA, the main impact for me has been that some sites and applications now prominently display the recommended language “Do Not Sell My Personal Information”—wording mandated by the California authorities.

As my comments imply, most companies have taken these laws as compliance exercises that they have been able to address with changes to their user interface—but not necessarily by improving their overall policies. For example, when I recently clicked

on a “Do Not Sell My Personal Information” link, the next page required that I provide my home address, and it wouldn’t allow me to submit the form because I don’t live in California. Not being a California resident, I could not request that the company not sell my personal information! While these laws will certainly enable a new generation of class-action lawsuits, it is too early to know if they will establish new data processing norms that need to be followed by ethical companies and organizations.

STALLINGS: Privacy officers in companies that do business in the European Union and California are responding to GDPR and CCPA, respectively. We will see technical implementations and policy changes put in place over time. The magnitude of the actual effect on consumer privacy is yet to be seen.

THAW: Of course they are having an effect—the question is whether they are having the desired effect. In the case of the CCPA, it’s just too early to tell. GDPR has been around longer but really is not at its core a security regulation. It is much more about providing individuals with notice, transparency, and control (to varying degrees) of the use, retention, and maintenance of certain types of their information. Security measures (obviously) need to be incorporated to implement these goals, but these are primarily privacy goals.

Regarding cross-jurisdictional enforcement and harmonization (or the lack thereof) among privacy laws—obviously, it would be “easier” if all the laws were the same. But that isn’t a very interesting statement. The more important question at the core of this issue is

whether or not there is a social benefit in allowing nations, states, or even regions to provide different levels of privacy depending on the desires of their local polities. It is certainly the case that given the vast differences among the diverse cultures of the world, we should tread lightly in asking for “global” harmonization. It also is likely the case that in any harmonized system, we should consider thoroughly whether we want to allow “smaller” units (a state within a nation, a city within a state, and so forth) to provide greater protections than those afforded by the “larger” unit.

WIJESEKERA: At best, compliance comes much later—perhaps through engineering innovations and the consequences of legal action after damage. Although the Internet or global access to information though other forms of human contact are bound by law, these laws are not universally binding nor universally enforceable nor do they use international treaties.

COMPUTER: Many cell phone apps are designed to monitor the user’s location at all times, not just when the app is in use, including many that have no reasonable use for location data. Users may not be aware of this type of monitoring. Should laws or regulations have more limits on what kind of, and how much, user information companies should be allowed to collect.

BISHOP: This really goes back to one of your earlier questions. The most widely adopted solution is to tell the user what data are being collected and how they will be used. Most users simply click “Accept” without reading the terms. Those that do read the terms often don’t understand them or their implications. Further, in many cases, companies can

unilaterally change the terms. Usually, when they do this, they have to allow users to opt out of information sharing—but that is “opt out,” not “opt in,” and the latter is always better.

DENNING: We might need more limits, but we also need better transparency so that users know what they’re getting into when they sign up for or use some service. That information should be clearly communicated to users and not buried in the fine print of privacy policies.

GARFINKEL: The problem with laws and regulations is that they are necessarily broad and not easily changed, so they always lag behind innovation. Many techniques that it might seem reasonable to ban today might be desired in the future if they are offered in a manner that is secure and respects user privacy and intentions.

At the same time, we have more than two decades of research showing convincingly that “informed consent” doesn’t work in most privacy-related situations. There are simply too many decisions requiring consent, and users rarely have the time, interest, and technical sophistication to be properly informed.

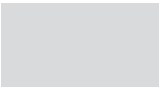
I think that one possible solution is to migrate away from business models based on harvesting and reselling personal information. The financial windfall of behavioral advertising never really materialized, and nobody likes having advertisements for mattresses follow them around the Internet for months after purchasing a new bed. Meanwhile, I believe that apps and services offered by governments, nonprofits, and community-based organizations will increase in popularity in the coming years.

STALLINGS: I’m not sure a lot more is needed in terms of regulations. I think regulations should lean more toward requiring opt in instead of opt out. And I think the list of rights and principles in GDPR is a good model for other regulations to adopt.

WIJESEKERA: Yes, but the question is enforceability (both technically due to attacks) and accountability.

COMPUTER: The pandemic spread of COVID-19 has upended societies around the world, often in ways that conflict with privacy. For example, Apple and Google announced that they are each developing application-programming interfaces but intend to integrate into their respective operating systems, for mobile devices they support, the capability to collect contact-tracing data. Will these intrusive capabilities become permanent features of mobile device operating systems, as they already have become in many mobile device apps? Even if users are permitted to opt in/opt out, can the operating systems and apps be hardened sufficiently to prevent unauthorized access to detailed user-identifiable, contact-tracing data by governments and others for purposes other than combatting a pandemic? Can corporations be trusted not to disseminate contact-tracing data with governments and other third parties beyond the originally stated scope of sharing?

BISHOP: I believe they will become permanent—it’s always easier to add something to a system than remove it. I also doubt if the operating systems and apps can be hardened sufficiently. If a government wants



that information, it has tremendous resources to get it; techniques used have included implanting spyware, for example. And as mobile devices are vulnerable to attack, the attacker may not be a government.

As far as trusting Apple and Google, I can't comment on the trustworthiness of either. In general, a good way to determine this is to look at how those companies, or any companies, react to authoritative regimes' demands for access to the data. Whether they comply, and if so how, will tell you a lot about how they value their users' privacy.

Also, remember that, in many cases, the user is not the customer of the corporation; third parties are. Often, it is advertisers, and the data collected about the user enable targeted advertising. This needs to be factored into how trustworthy an entity (corporation, government, and so on) is.

DENNING: It isn't enough to just trust that companies and the government will get it right. We need to make sure that the technology being developed and deployed is responsive to our security and privacy concerns. This might require new policies and laws regarding contact tracing. Whether contact-tracing apps become permanent will depend on how useful they turn out to be.

GARFINKEL: The "intrusive capabilities" described in the question are already permanent features of mobile device operating systems, and they are not opt in/opt out, they are widely available and deployed. For example, in 2018, *The New York Times* documented how fine-grained geolocation data for many cell phone users are being collected and archived.⁶ Today, there are multiple systems that

capture time-based geolocation data on the typical cell phone, each corresponding to a different advertising network.

The question facing platforms and users is whether application-specific contact-tracing technology should be deployed and what should be done with those data. This is a public policy decision, not a technology question. To be effective, these systems should be mandatory, and the collected data should be integrated into existing public health contact-tracing programs. That's because technologies like Bluetooth may overestimate a person's contacts: Bluetooth might think that people on opposite sides of a plastic barrier or a window are standing next to each other. Meanwhile, these systems are likely to be hacked by individuals and nefarious organizations in ways that are not apparent when they are being designed.

As for the question of whether specific companies can be trusted to act in a manner consistent with their public statements—the definition of a trusted system is one that can violate your security policy without you having recourse. Of course, these companies can be trusted. We should ask: *should* these companies be trusted?

STALLINGS: Lots of questions! The answer is "be pessimistic, be very pessimistic."

THAW: I don't think anyone "knows" whether or not contact-tracing apps will become "permanent" features. It is just as easy to write a law limiting such permanence as it is to write one that never expires. Legislatures will confront these questions, and they should think carefully and seriously

on what mechanisms (for example, sunset clauses) they wish to put into their laws to limit the likelihood of continued use past the original justification. Furthermore, legislatures should think carefully on the scope of use and whether to adopt language prohibiting the use of collected information for any other purpose. This is not unprecedented—in the United States, for example, similar legal limitations exist on the use of U.S. census data and on data collected in the course of background investigations.

WIJESEKERA: Yes, once the genie is out of the bottle, there is no putting it back in, and more applications of this kind will start to evolve and be enhanced. Trusting a company does not matter as much as the effects caused by legislative incoherence where different localities interpret the same application as providing healthy practices for the community (where, of course, the definition of the community varies due to time, cultural differences, and immediate needs) or as a privacy violation.

COMPUTER: Five years from now, will we still be asking the question: is it security *and* privacy, or security or privacy?

BISHOP: Yes.

DENNING: I didn't know it was ever a question. My interest in security, starting almost 50 years ago, was driven by a desire to design mechanisms that would protect private data from reaching unauthorized persons.

GARFINKEL: I honestly don't think that many people are asking this


question now. For most readers of *Computer*, I suspect there is wide belief that both security and privacy are achievable goals. Meanwhile, I think a growing number of nontechnical people believe that both security and privacy are unattainable.

STALLINGS: On the level of technical implementation and system design, it will always be a question of how best to implement both security and privacy. All these other issues we've been discussing have to do with the demand for privacy on the part of PII principals, the level of enforcement of regulations, the amount of risk imposed on organizations for violating privacy, and so forth. But as to the actual question, security and privacy are both important, by and large compatible, and doable.

THAW: I hope not. After 20 years of listening to variations on "security versus privacy," when the question is overwhelmingly really asking about "surveillance versus privacy," I admit I'm skeptical that this debate will change. But I continue to hope.

WIJESEKERA: On the industry side, there will be contributions to privacy-enhancing technologies and cybersecurity enforcement mechanisms. Both sides will keep the issue alive. On the academic side, as long as *h*-indices and other such tangential metrics govern academia and its offshoots, we will do our best to keep all corpses alive as they advance some peoples' superiority over others. If and when these interests converge to a fixed point is difficult to envision, but I do not anticipate them converging within a decade.

The panelists in this virtual roundtable provided us with a deeper understanding of the correspondence between security and policy. It was interesting to see that the panelists had similar perspectives. We hope the outcome of this panel will help technologists better address the interrelationship between security and privacy in the engineering of systems upon which society depends.

We welcome your feedback on *Computer's* virtual roundtables. Last but not least, we thank the participants of this virtual roundtable. 

REFERENCES

1. A. Avižienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Depend. Sec. Comput.*, vol. 1, no. 1, pp. 11-33, 2004. doi: 10.1109/TDSC.2004.2.

2. J. Voas, "Software's secret sauce: The "-ilities" [Software Quality]," *IEEE Softw.*, vol. 21, no. 6, pp. 14-15, 2004. doi: 10.1109/MS.2004.54.
3. D. J. Solove, "A taxonomy of privacy," *Univ. Pa. Law Rev.*, vol. 154, no. 3, pp. 477-560, 2006. doi: 10.2307/40041279.
4. S. Garfinkel and M. Theofanos, "Non-breach privacy events," *Technology Science*, Oct. 9, 2018. [Online]. Available: <https://techscience.org/a/2018100903/>
5. "Universal Declaration of Human Rights. Final authorized text," United Nations General Assembly, 1952. [Online]. Available: <https://www.bl.uk/collection-items/universal-declaration-of-human-rights>
6. J. Valentino-DeVries, N. Singer, M. H. Keller, and A. Krolik, "Your apps know where you were last night, and they're not keeping it secret," *NY Times*, Dec. 10, 2018. [Online]. Available: <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>

DISCLAIMER

The views and conclusions contained herein are those of the panelists and authors and should not be interpreted as representing the policies or endorsements, either expressed or implied, of their employers. The U.S. Government is authorized to reproduce and distribute reprints for government purposes, notwithstanding any copyright annotations thereon. Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the authors or their employers, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

JAMES BRET MICHAEL is a professor in the Naval Postgraduate School's Computer Science and Electrical and Computer Engineering departments. He is a Senior Member of the IEEE. Contact him at bmichael@nps.edu.

RICHARD KUHN is an associate editor for *Computer*. He is a Fellow of the IEEE. Contact him at rick.kuhn@ieee.org.

JEFFREY VOAS is the editor in chief of *Computer*. He is a Fellow of the IEEE. Contact him at j.voas@ieee.org.