4

PROTECTIONS

WHAT'S TO BE DONE ABOUT PRIVACY IN THE DIGITAL ERA? THIS problem has vexed policymakers since the invention of the Internet, and there is no single, simple answer. In fact, it is likely that "privacy"—as it was defined in the past—will never be the same again, no matter what we do at this stage. But there certainly are things that we can do to address some of the privacy issues we all face, whether we were born digital or not.

For young people, there are two main problems, each of which merits attention. They are problems for all of us, but for those who were born digital, the effects will be compounded over a longer span of time. One of the problems relates primarily to the young person's identity; the other relates to her digital dossier. Each problem has its own contours and requires its own solutions. Despite reform efforts, existing law does not provide the answer for either of these problems if we mean to protect the privacy of youth in anything like the fashion in which we've protected the privacy of our citizens in the past.

Any solution to the problem of privacy is going to require the involvement of multiple actors. With respect to the first set of data—the data that make up the young person's identity—the person most capable of doing something about it is the young person herself. Her parents, peers, teachers, and mentors also have an essential role to play. And the companies that provide the services she uses, or stores the data she transmits, have a part in improving the situation, too. Finally, the state can do something to help by using its regulatory authority or influence on the law.

The young person herself is not in a position to solve the problem completely, but she can sharply mitigate any potential harm through her own behavior. Research we conducted together with our Berkman Center collaborator and friend Sandra Cortesi shows that many young users of digital technology have already developed commonsense strategies for addressing privacy issues and managing their reputations. We have often heard statements like the following in our conversations with young people:

> Male 1, age thirteen: "I realize that whatever I post online, I should be comfortable with everyone in the world seeing it."
> Female 1, age twelve: "If it goes online, it never comes back."
> Male 2, age thirteen: "Once it's on the Internet, it's there forever."

With that in mind, many of the young people we have interviewed use a mix of approaches for managing their privacy online. Some of them restrict access by adults to their social media sites. Others change their name on Facebook so that their friends can view their posts, but others cannot connect the posts to them personally. Privacy settings are also a key mechanism among youths for managing their personal information, and a majority of our focus-group participants expressed confidence that they adequately managed the disclosure of personal information.

But here's the most interesting finding from this research: when it comes to reputation management, young people don't rely so much on controls like privacy settings when they post something online. Rather, they often think carefully *beforehand* about whether or not to share a

given piece of information at all, and if so, over what platform. Many young people are beginning to use this type of logic, often after having a bad experience or hearing of a friend's. Some young people we have met are likely more sophisticated in their thinking about privacy than many adults, not less. In other cases, young people are at risk because they make poor decisions on a daily basis.

Obfuscation is another strategy that young people sometimes adopt to protect their own privacy. Obfuscation means deliberately using ambiguous, confusing, or misleading information when interacting with digital technology to interfere with excessive data collection practices.[1] Consider, for instance, the use of AdNauseam, a browser plug-in that automatically clicks on all blocked ads in the background as a user surfs the Web—preventing ad networks from building up detailed user profiles based on someone's otherwise selective, and therefore revealing, clicks.[2] Another example is CacheCloak, which enables real-time location privacy for mobile users by "confusing" location-based services, deliberately hiding part of the user's path by mixing it with surrounding users' paths.[3] Though promising, these two examples indicate that the most effective obfuscation strategies currently require a relatively high level of digital literacy. Such self-help approaches are available only to the most tech-savvy users.

Young people can also help solve the problem of privacy by educating one another. There is evidence that children already do educate each other about online protocols. In focus-group interviews, young people shared with our research team how they sometimes turn to their tech-savvy friends when in need of help:

> Female, age thirteen: "[Needing help online] doesn't really happen to me very much? But if it was something that was really, really difficult, I feel like I'd ask that kid at school who's really smart with technology."

One of the most promising solutions to the privacy problem is to emphasize peer-based learning and activism. Young people are social, connected, and resourceful. There is good reason to believe that youth

have the capacity to work together to effect change with respect to their online environments. Whether it is Facebook, Snapchat, or Google, many tech companies periodically experience the power of tens of thousands of young people expressing their dissatisfaction in a concerted way via the very platforms these companies provide. These incidents are often a response to new versions of a company's privacy policy or terms of service.[4] More often than not, these types of protests result in some sort of "Thank you, and we're listening," message shared over the site's official blogs by senior executives.[5]

Parents and teachers have an important role to play in educating young people about privacy and protecting their identities. When discussing privacy-related decisions about posting content in our focus groups, young people often mentioned parents and family members as sources they asked for advice. This role needs to start with modeling smart behavior. Almost inevitably, parents also disclose information about themselves online that they come to regret. On the other extreme, some parents and teachers have no online identity, and it is hard for the adults in this group to establish credibility on the topic with their children or students, particularly if the latter are tech-savvy. In our interviews, several young people expressed skepticism when it came to their parents' knowledge about privacy and social media. ("My parents are not super great with computers, so I don't think that that would go so well."[6]) The first step for parents and other adults must be to engage in life online in constructive ways. Though often awkward at first, conversations between parents and their sons or daughters about identity and privacy online are essential—exactly *because* of their different views on privacy.[7]

Parents often wonder whether they should track their children's activities. It is relatively easy for parents to monitor at least certain aspects of their children's online activity, particularly when they are younger—there is special software designed to assist in this very task, such as Spector Pro or Net Nanny. The use of smartphones, though, makes it harder for parents to keep taps on their children's online behavior—harder, but not impossible, given the availability of next-generation software that does allow monitoring of children's smartphone usage. (The Korean

government even tried to mandate the installation of such software.) From a parent's perspective, there might be an instant appeal to this approach: parents want to know what their children are up to online, especially when they're younger, and parents want to have a sense of who is communicating with them.

But it is definitely worth taking a step back and thinking hard about the use of such technology. Tracking young people's online activities is likely to undermine trust between parents and their children, as we discussed in chapter 2. Our research shows that there is a great likelihood that children will get around the controls anyway, whether at home or elsewhere. It's also helpful listening to the young people themselves. Many young people say that when they know their parents are watching what they do online, they censor themselves and chat less on instant-messaging apps, or choose not to access their personal social media accounts on a shared home computer. The most heavy-handed online surveillance and tracking techniques that parents use in the home typically backfire. Young people are using services like WhatsApp, Snapchat, or the chat functions in multiplayer games often because they feel alienated in other public spaces.[8] The answer is not to keep chasing them away from safe spaces into more remote zones.

One important, and often more effective, alternative to the idea of tracking, at least for parents of young children, is to go online together and make it a shared activity where possible—whether it's sharing a laptop screen on the sofa in the living room, or letting children play their favorite YouTube videos on their own smartphones when hanging out together over a hot chocolate in a coffee shop.[9] Parents might also show young people how ordinary browsers on laptops and tablets, or the apps on their smartphones, track online activities. By watching their parents track their digital traces using built-in tools, children can see how easy it is for people to track their online activities on virtually any device.

Instead of relying on parental controls and monitoring tools, parents should focus on building trust over time. Certainly, there's a place for knowing what your young children are up to online. Parents might consider limiting access to the Internet when their children are very young, but then allowing for increasing independence as they grow older.

Children can in this way prove themselves to be mature enough to venture online without constant supervision.

Teachers, too, have a strong influence on the privacy attitudes and behavior of young people in the digital age—perhaps even more so than parents. In many conversations with young people, our research team found that young people respected their teachers' knowledge and understood that teachers were looking out for their best interests. The notion that teachers can be a source of knowledge is also supported by other studies: 70 percent of online and cellphone-using teens have "gotten advice about internet safety from teachers or another adult at a school," according to one survey.[10] However, although the children we interviewed did not mind receiving advice from their teachers, they were reluctant to be "friends" with them or have teachers follow them online. According to one survey, 30 percent of teens online have teachers or coaches as friends in their network, but most participants expressed discomfort with the idea of being friends with current teachers.[11] This quotation from a fourteen-year-old participant captures the concern of many young people well:

> I think I wouldn't [become Facebook friends with my teachers], just because I'm such a different person online. I'm more free. And obviously, I care about certain things, but I'm going to post what I want. I wouldn't necessarily post anything bad that I wouldn't want them to see, but it would just be different. And I feel like in the classroom, I'm more professional [at] school. I'm not going to scream across the room, "Oh my God, I want to dance!" or stuff like that. So I feel if they saw my Facebook they would think differently of me. And that would probably be kind of uncomfortable. So I probably would not be friends with them.

In addition to giving advice on an ad-hoc basis, it is important for teachers to instruct their students in digital literacy in the classroom and in informal learning environments. Broadly defined, digital literacy can be understood as "the ability to effectively and critically navigate, evaluate, and create information using a range of digital technologies."[12]

Schools in the United States have slowly been adopting digital literacy programs as part of their curricula, and many have begun integrating them more thoroughly into their pedagogical frameworks.[13] Teachers and administrators are not alone in these efforts. Several organizations, including Common Sense Media, have rolled out entire privacy curricula or modules to support teachers in these efforts. Our home institution, the Berkman Center for Internet & Society at Harvard, has participated in and contributed to such efforts, both domestically and internationally, and has designed a curriculum to teach digital privacy and safety fundamentals to middle-school and high-school students.[14] It aims to help them to understand digital privacy and safety as well as related concepts such as personal reputation; to reflect on why and how digital privacy and safety matter in their own lives; and to become familiar with the primary challenges and opportunities they are likely to encounter online in social, educational, legal, and other contexts.

The third concentric ring out—beyond young people themselves and their parents and teachers—is the technology companies, which also have an important role to play. Companies can make a great deal of difference through stronger site design. Several companies, including Google and Facebook, have introduced better user interfaces, designed privacy dashboards, and provided check-ups that make it easier for youth to make good choices about personal data. Over the past few years, some of the world's leading social media companies have vastly improved the controls young people can use to keep unwanted viewers from accessing information about themselves and their friends. On Facebook, for example, users (young and old alike) now have an easy way to determine the reach for every single piece of content before they click "post."

Many tech companies—and especially app developers—still have a long way to go. They need to step up and work hard to empower young users to make better privacy decisions. The environment of light regulation in which they operate in the United States is predicated on their commitment to earning and maintaining the trust of those users. These companies, including but not limited to social media platforms and app developers, need to be more explicit about what they will do with user

data, how long they will keep the data, and how users can go about deleting data about themselves. The temptation for these companies has been to maintain maximum flexibility, so that they can mine the data they've collected to support future revenue streams. From a public policy standpoint, however, that approach is wrong. The paradigm needs to shift from a firm-centric model, where companies choose what to do with user data, to a user-centric model in which ordinary people—not just the most tech-savvy—can manage their own data.

Some companies have begun to understand the need for a paradigm shift as they seek to broaden their reach to younger children. Google's announcement of a dedicated YouTube app is a case in point, although with some significant flaws.[15] Launched in the spring of 2015, the non-login, mobile-only YouTube Kids app is part of a growing ecosystem of platforms that can be used by parents to let (even very young) children watch videos. Its control features give parents a tool to decide what the appropriate screen time for their children should be and to limit search options. Most importantly, from a digital identity perspective, the product was launched as a "sign-out" application (as opposed to "sign-in"), which means it doesn't allow the collection or sharing of personal information. This YouTube app can't be linked to a Google account; nor can videos be uploaded or comments added, which might otherwise reveal personally identifiable information. And the ads don't lead to third-party websites; clicking on an ad won't take users anywhere.[16]

Even more powerful than what an individual tech company can do is what an entire industry might be able to achieve. In one promising example, a large number of educational technology (ed-tech) firms teamed up to improve privacy for children through the K–12 Student Privacy Pledge. Announced in late 2014 by the Future of Privacy Forum and the Software & Information Industry Association, the initiative brings together more than two hundred K–12 school service providers—including tech giants Microsoft and Google—to safeguard student privacy based on a series of principles. The commitments should lead to a reduction in the number of data points that are added to a young person's dossier, as the pledge limits data collection and use to what is needed for

authorized educational purposes. It also limits the type of personal profile that can be built for a student with data that supports educational purposes and that has been authorized by the parent or student. This initiative may also help students with digital identity management: the signatories have agreed not to sell or otherwise disclose student personal information collected through an educational or school service for behavioral targeting of advertisements.[17]

The place of the law may not be immediately obvious in the context of information that a young person discloses about herself. If someone decides to disclose information about herself online, the checks on that behavior should be imposed by friends, family, or teachers, not by the state. However, the state does need to provide a crucial backstop, and in the United States, this is already happening to some extent. If a company says that it will do one thing, and it does another, then the Federal Trade Commission (FTC) can hold the company responsible for its actions. This type of enforcement mechanism is crucial and, if anything, should be increased, in light of the fact that the FTC is constantly understaffed and underfunded for its broad-based enforcement efforts.

In the same vein, the law could also mandate clear, simple labeling of privacy policies. The state requires certain consumer food products to have a standard label listing the nutritional facts about the food: in the same manner, the state could make it easier for users to manage their online identities by requiring online services to provide clear, standardized labeling for their privacy policies. An icon-based system, making the most important aspects of the site's privacy policy clear (such as how long data is stored before it is deleted), could go a long way toward ensuring that young people at least know the full extent of the consequences they will face when posting online content. This need not be through new laws[18]—in theory, an industry consortium could take up the same charge without a state mandate. But to date, this has not happened on a large scale. In the meantime, the lack of clarity about how companies treat personal information is a growing problem for youth—not to mention for everyone else living in the digital era.

In addition to setting minimum standards or requiring better information on site practices, the law could also come into the picture to help *after* information has become part of a young person's identity. Currently the most powerful—and certainly the most controversial—legal approach to this issue is the "right to be forgotten." Legal scholars, courts, and legislators around the world are still debating the exact contours and different aspects of this relatively new idea; in essence, it encapsulates the notion that people have a right to have data from their digital dossiers deleted if certain conditions are met.[19]

A version of this right made headlines in 2014 when the European Court of Justice (ECJ), the highest court in the European Union, handed down its verdict in a landmark privacy case known as the "Google Spain Case."[20] In short, the court ruled that any person has the right, under certain conditions, to ask a search engine operator to remove a link to a webpage when his or her name is used as a search term. This decision applies to situations in which the information is inaccurate, inadequate, irrelevant, or excessive, even when the publication of the information itself was perfectly legal. The court made clear that such a right to be delisted—or, in European terminology, the "right to informational self-determination"—isn't absolute and must be balanced against other rights, including freedom of expression. The court provided little guidance on how to engage in such a balancing act, however, and left it largely to the search engine companies themselves to come up with a strategy on how to implement the ruling. By the end of December 2015, Google had received more than 360,000 requests and evaluated more than 1.2 million URLs for removal. Google actually removed 42.2 percent of those 1.2 million URLs from search results, including many from Facebook and YouTube pages.[21]

The ECJ ruling, along with new legislation that harmonizes the right to be forgotten across EU member states, has received harsh criticism in the United States owing to freedom-of-speech concerns. However, similarly spirited efforts have also emerged in the United States. Particularly relevant in our context is California's "Online Eraser" law, effective since January 2015. In essence, it gives a minor who is registered on a website, online service, or mobile app that is directed toward users under the age

of eighteen a right to request the removal of information she previously posted.[22] However, this right to wipe away past content doesn't cover what others—for instance, friends—have posted, and is therefore of limited help to a minor who is attempting to manage her digital identity. The legality of the Online Eraser law, and its scope and effectiveness, are still highly contested.[23]

There is even more to be done when it comes to the second challenge, protecting the privacy of young people with respect to their digital dossiers. This challenge is greater than the challenge of managing online identity because there is much less that the young person and her family can do to solve the problem directly. And the challenge is doubled because many of the economic incentives at work encourage precisely the wrong actions.

A young person and her friends and family can't do much on their own about the information that third parties collect about her, let alone influence what third parties do. She can limit the amount of time she spends online or in places where data will be collected about her, but all roads seem to lead to a more—not less—digitally connected existence for young people. And she can only be so careful. When it comes to her credit, she can call up Experian, TransUnion, or Equifax to ask about the data they've collected on her, if she lives in the United States. For other kinds of data, there is no simple mechanism under the law for her to use. Medical records, school records, records of where she goes online and the purchases she makes, all are pretty much unavoidable in our digital world.

Young people generally have very little idea what is being collected about them by third parties. One high-school student explained how confusing this lack of control can be:

> So I don't know how I feel right now just because I feel like anyone can have access to your stuff. And do you accept that because you participate in using the Internet and technology like that, or is there a way to fight that and create ways in which you can keep stuff

> private and keep stuff yours? . . . So, I mean, if you give people a situation, in terms of, "this is this, and you have to accept this if you choose to do this." Fine, but . . . Google . . . they don't tell people, "Oh, we track everything you do." Especially with youth. People Google everything because they just think to. They don't know, where this information goes. They don't know that when you log on to certain sites, they keep track of when you log on and what you write. So, I mean, I don't know. It's the fact that people don't know. . . . There's not enough transparency for young people to know and they participate very unknowledgeable. That's what scares me because you don't know what that will end up looking at later on.[24]

The problems that come from the existence of digital dossiers can be mild—the targeting of advertisements in ways that are arguably attractive to Internet users—or they can be terrifying—in the case of identity theft, stalking, or denial of a job because of what someone found in a digital file.

With respect to data breaches, there's little or nothing that a single person can do. And parents and teachers are just as powerless to help youths as they are in helping themselves in this regard. Ordinary citizens could do nothing about the breaches into Acxiom, Home Depot, or even the US government.

Technology companies and law enforcement authorities have critical roles in this area, as do those who collect data about youth. Technology companies that create the systems to collect and store data about individuals have an obligation to build secure systems, and they ought to be held accountable under the law when they do not. In the United States, the FTC has played a key role in holding companies accountable. Services like social media platforms and Internet Service Providers (ISPs) ought to tell users what they collect about them—for instance, the "clickstream data," which details information about where one has surfed online—and they ought to report who will receive and utilize that data.

More can and should be done legally on behalf of young people to help them safeguard their growing digital dossiers. Although the law

cannot solve the privacy problem on its own, well-designed laws can do a lot of good. They can help protect the privacy of youth by limiting the collection of data about them in the first place, for example, and they can establish principles for how data, once collected, should be treated. A good example has been set by the efforts to protect student data in the United States when students use online resources for school projects. Educational institutions have adopted all sorts of digital technologies and entered into privacy-protection agreements with ed-tech companies, and state legislators have introduced new laws (over 180 bills so far) regulating the collection and use of student data.[25] California's Student Online Personal Information Protection Act (SOPIPA) served as a model for other states in governing the activities of website operators, service providers, and mobile app developers that design and market products for K–12 educational users. The act bans practices such as targeted advertisement and prohibits the use of information collected over these services to create student profiles except for authorized educational purposes.[26]

Finally, the law can make an important contribution by ensuring that certain protections kick in when personal information has been involved in a security event caused by criminal hacking, leaks by insiders, unintended disclosure, lost flash drives, and the like. Security breach notification laws in the United States, and more recently in Europe and other parts of the world, require private, government, and educational entities to notify individuals within a certain time frame about data breaches that come to light.[27] By requiring notice, these laws give persons who may have been affected by a breach warning that their personal information has been compromised, providing them with an opportunity to protect themselves against identity theft and other negative consequences.

In designing legal solutions to the problems presented by digital dossiers, it would be a terrible mistake to lose sight of the fact that the world is more connected than ever before. A violation of a young person's privacy may have ramifications far beyond his or her immediate community. Data about young people freely cross geographic and political borders. A young woman may well be doing business with companies

based in other countries that provide online services to her; that's certainly true if she is a European or an Asian person using a US-based system. The problem is that the protections she enjoys in one country may not protect her in another context online. Any set of solutions that we come up with must take account of these cross-border considerations.[28] The invalidation of the so-called Safe Harbor agreement by the ECJ, which allowed US companies to transfer European citizens' data to the United States after completing a self-certification process, hinted at the challenges involved when developing global privacy standards. Our interconnected world is still governed by very different national privacy laws and values.[29]

It is also important to bear in mind the costs of privacy regulation. To date, privacy laws have come not only with high costs, but also with flaws in design and implementation. Privacy protections sometimes run up against free-speech rights, as there are many instances online where one person's (or company's) speech may violate another person's privacy.[30] Consider, for instance, a case in which a young person created a website where she posted pictures, names, and cellphone numbers of her classmates online in order to create her own social network site. Under European data protection laws, her activity, regardless of its good intentions, may be illegal. But this is not the case in the United States, where free speech in many instances trumps privacy. American laws have yet to catch up to changes in the way that youths are leading their social lives in networked publics.

Moreover, we must be careful not to make things worse when designing privacy legislation. Badly designed laws can hamper innovation. Many new applications and services are premised on the notion that people want to aggregate their personal data in a single place online. Social networking sites are one way to do this. But it is easy to see how less regulation might allow entrepreneurs to experiment with new business models, and in turn possibly create jobs and economic growth in markets around the world. Conversely, the existence of an appropriate legal framework that protects privacy could be a fundamental trust-enabler in the digital economy. Several studies conducted in the aftermath of the Snowden revelations in 2013 taught us how privacy

invasions—here in the form of extensive, secret surveillance activities by the US government—absent robust legal protections eroded trust in leading tech companies. Analysts estimated that the Snowden leaks cost major US technology companies billions of dollars in lost sales.

In response to revelations about government surveillance, several major tech companies, including Apple, Google, and others, announced their plans to enable default end-to-end encryption in certain applications on smartphone operating systems. Law enforcement and intelligence communities in the United States immediately expressed concerns about this trend, arguing that it could inhibit the government's ability to access communications in circumstances satisfying Fourth Amendment search-and-seizure requirements. Similar arguments have been presented against strong legal protections of consumer privacy, which can make it tougher for law enforcement personnel to do their jobs. From our perspective, both concerns are legitimate, but both also tend to be overblown, given the technological realities (in the case of encryption)[31] and the long catalog of limitations and exemptions that are typically written into privacy laws.

In the post-Snowden era, there can be little doubt that we have to examine our current legal regime critically—and might even be in need of a new legal order—if we are serious about protecting young people's privacy rights. However, there is substantial disagreement among policymakers, companies, users, and even experts around the globe over what exactly the next generation of (new or updated) privacy laws should look like. Privacy advocates have called for omnibus data-protection laws—overhauls of the law that could conceivably seek to protect every aspect of personally identifiable information across the private and public sectors. The European Union recently passed a comprehensive law called the General Data Protection Regulation (GDPR), which should come into force in 2018. It builds and expands upon the Data Protection Directive of 1995 that harmonized national privacy laws across member states, but it did not address more recent technological developments, such as social media, Big Data, or cloud computing, among others. The United States has taken a different approach to privacy law through sector-specific legislation.[32]

The various possible designs of privacy laws come with different advantages and disadvantages. An omnibus approach to data protection law, such as Europe's GDPR, for instance, enhances user privacy by raising awareness and by providing a minimum level of protection, especially where more specific legislation has not been enacted. However, the merits of such one-size-fits-all laws remain contested. Critics argue that omnibus data-protection laws tend to be cumbersome, bringing with them unintended consequences and very high transaction costs for businesses, while benefits remain unclear to end users.[33] Sector-specific privacy laws, in the tradition of the United States, in contrast, are necessarily more narrowly tailored and more specific. The sector-specific approach might leave more room than the omnibus approach for experimentation with innovative forms of information and privacy regulation, including multi-stakeholder approaches and private-public partnerships. A possible downside is fragmentation, which might increase compliance costs for companies (for example, with the various state-level security breach notification laws mentioned above). Another possible disadvantage is that sector-specific laws might create competitive disadvantages for companies that fall under it.

While it is too early to declare either approach to be more effective than the other, several overarching principles are clear. First, laws should let users, not corporations, decide what happens to data about them. This is the key lesson that we can learn from European-style privacy laws: they put the individual in control of his or her personal data. This approach to privacy has been less popular among lawyers in the United States than among Europeans, but it has recently received much attention at US technology firms working to find better ways to protect online privacy. The most powerful change that we could make in privacy protection would be to shift to user-centric privacy controls. This route would also entail providing adequate support to users in their efforts to maintain these controls. Instead of thinking of personally identifiable data as the "property" of those who collect it, we should shift the focus to those to whom the data relates. There is no incentive for companies to change the paradigm on their own, absent legal intervention.

Privacy laws should also make it easier for people to protect themselves once they decide to disclose personal information. A reasonable approach would be to require companies that collect data on a massive scale, like Experian and Acxiom, to produce reports about consumers upon demand, much as the credit-reporting agencies do, in a standard, understandable format. The FTC recently made a series of legislative recommendations along similar lines.[34] New business models for intermediaries to help users manage their data might emerge as analogs to MyFICO and others in the context of US credit reporting. It may be tricky to determine who is subject to the rules and what they are required to report; however, these questions could be addressed in well-designed legislation. The downside would be the costs to the companies that collect the information, which might well drive some of them out of business. But the interests of these particular businesses are outweighed by the growing importance of enabling users, including young people, to control what others can come to know about them.

In addition, the law should do a better job of protecting consumers from data breaches before they occur. It should make clear what it means for an actor who collects personally identifiable information to be negligent in terms of computer security. Companies that store information about users should be held to a reasonable standard for maintaining the security of their data collection and storage systems. In the event of a data breach, an individual or a class of persons should be able to hold companies accountable for the breach. If companies do not meet this reasonable standard for security, they should be held liable.[35] Today, these companies often get a free pass when they allow a breach. We realize that this change may require judges to call upon the expertise of computer security experts to determine a reasonable standard—but that sort of expertise is required by courts all the time. The lessons learned from over fifty data security–related law enforcement actions taken by the FTC could also inform the definition of appropriate standards and best practices.[36]

Finally, we must recalibrate the law's current focus on collection practices and begin a serious debate about the legal restrictions we may want

to place on certain uses of data. Traditional privacy principles restrict the uses of data either to those required by law to have it or those to whom the individual has given consent for its use. Such a narrow definition threatens important health research, fraud prevention practices, and many of the benefits that emerge from Big Data analysis.[37] Where should we draw the line of permissible uses and those we are not willing to accept? To answer that question, we need to think not only about uses that cause financial or reputational harm, but also about perfectly legal uses that nonetheless cause discomfort.

The law needs to be amended to protect the privacy of young people better than it does today. But we also have to acknowledge that law-based approaches to digital privacy comes with a series of challenges and limitations. The global nature of the Internet is central to this problem. Even if Google's engineers in California behave appropriately when it comes to a young person's data and treat that data with respect, it is entirely possible that someone in another country will gain access to the same data and disclose it to the individual's detriment. Effective solutions to the digital privacy problem will not only have to be nuanced, they will have to be global. We also have to accept that the law often cannot keep up with today's rapid evolution of digital technology and changing user behavior. We run a real risk that the privacy laws we draft today will immediately become outdated once they are enacted. Finally, we must acknowledge that well-intended but overly broad or badly drafted laws can do more harm than good in the quicksilver technology environment in which we live.

Young people—who live so much of their lives in networked publics—are unlikely to see privacy in the same terms that previous generations have seen it. In the context of US law, we have relied upon classical distinctions between "public" and "private." Now that line has become blurred, especially for our young people, and the traditional legal mechanisms are not working as well as they have previously. A similar shift has occurred in the copyright environment: it has become so easy to make a copy of a creative work, and social norms for doing so are so strong, that a chasm has opened up between what the law says and what youths do. The traditional legal definitions and mechanisms, in the

privacy context as well as in the intellectual property context, fit awkwardly when changes of this magnitude occur.

The implications of this misfit will only grow as young people continue to live more and more of their lives online. In this period of transition, as we rethink how the law should work, those who can do something about it—online technology companies, as well as parents and teachers—need to take on greater responsibility in helping young people make good choices about their personal information in networked publics.[38]