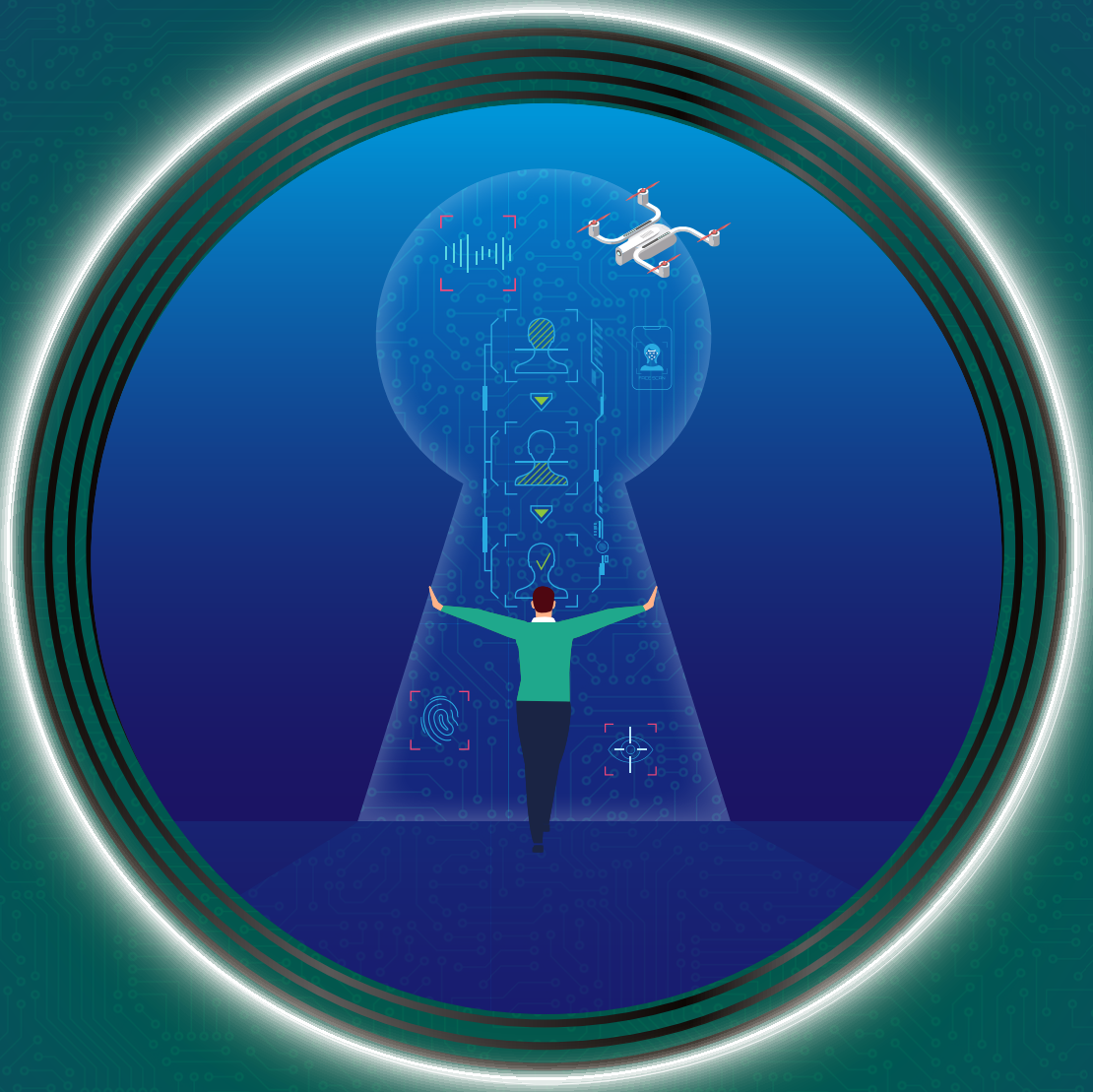
Deloitte. Insights

A report from the
Deloitte Center for Financial Services



Reimagining customer privacy for the digital age

Going beyond compliance in financial services

Contents

Getting smarter about privacy

> "New technologies are radically advancing our freedoms, but they are also enabling unparalleled invasions of privacy."[1]
>
> — Electronic Frontier Foundation

Customer privacy has become an increasingly complex and contentious topic, as the tools and technologies capturing data about every facet of our lives have proliferated. Many consumers now believe they no longer have control of information about themselves[2] and are starting to pay closer attention to how information about them is collected.

Such concerns are impacting the financial services industry as well, where customer data has always been a core asset. Long before data became the oil that fuels the digital economy, financial institutions have safeguarded customers' private information and used this data at macro and micro levels to serve clients.

In light of recent regulatory developments, such as the General Data Protection Regulation (GDPR) in the European Union, and advances in technology, customer privacy is becoming an even more intricate challenge—for individuals whose information is at stake, for companies that are expected to protect this information as well as use it responsibly, and for regulators charged with consumer advocacy who are playing catch-up.

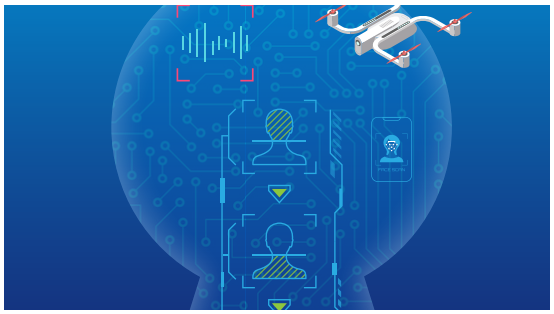
Many regulators around the world are taking unprecedented interest in privacy.

In fact, many regulators around the world are taking unprecedented interest in privacy and have begun to establish new rules. GDPR is arguably the most notable of the latest developments, offering EU citizens sweeping protections to their personal data. Under GDPR, all companies that handle EU consumer information—including financial institutions—must obtain express opt-in consent to collect their data and promptly notify citizens of data breaches, or risk paying steep fines. Consumers also have a "right to be forgotten," a stipulation that requires companies to erase all personal data currently maintained upon request or if the data no longer serves the original business purpose.[3]

The United States, meanwhile, does not have an all-encompassing rule like GDPR. US federal regulations tend to be narrower in scope and generally only protect specific types of data or are sector/industry-specific (see Appendix on page 15 for a summary of federal financial privacy laws).

Some trade groups, such as the Association of National Advertisers[4] and the Internet Association,[5] have begun to advocate for an all-encompassing federal privacy law like GDPR to avoid having a patchwork of legislation. Lobbyists, too, are beginning to speak up. In 2018, the US Chamber of Commerce called on Congress to adopt a federal privacy framework "to provide certainty and consistency to consumers and businesses alike."[6]

In the meantime, the lack of a single, federal mandate has placed the onus on states to craft their own privacy laws. For example, California passed the Consumer Privacy Act in the summer of 2018, granting consumers sweeping control of all forms of their personal data[7] from traditional identifiers such as addresses and phone numbers, to nontraditional data sources such as "likes" on social media or interactions with personal assistants. Other states, such as Delaware[8] and Vermont,[9] have recently enacted their own



The rapid penetration of digital technologies into almost every sphere of life has revealed how fundamentally limited privacy protections conceived for the analog age are today.

privacy laws. As consumers demand more control over their personal data, even though many may not be familiar with existing privacy regulations, more states may follow suit.[10]

Adding to this regulatory uncertainty, today's digital innovations are also reshaping the notion of privacy in unexpected ways. The rapid penetration of digital technologies into almost every sphere of life has revealed how fundamentally limited privacy protections conceived for the analog age are today.[11] Our ideas about privacy—what information should be considered private and what should be done to protect one's privacy—are fast evolving with new digital technologies and the new data they generate.

This situation is further exacerbated by the fact that privacy has no single, universal definition. In fact, several privacy scholars have noted that the very idea of privacy today is "a concept in disarray,"[12] "embarrassingly difficult to define,"[13] and "an essentially contested concept."[14] This challenge is due, in part, to the fact that privacy is not just a social value and "a good to be achieved," but also a right, with legal ramifications.

There is also debate about data ownership (*whose data is it?*) and data stewardship (*who can best safeguard customer data?*).[15] Both of these challenges have no easy answers.

One can only imagine the breadth and complexity of privacy issues that may be faced a decade from now, when most human interactions, even those now considered private, could be exposed for others to collect, mine, and share. Indeed, could privacy become a "luxury," as discussed during a panel at the World Economic Forum's Annual Meeting?[16]

Managing privacy in this ever more data-centric world could require new thinking. In this report, we will discuss the following conundrums:

- What should financial services firms do to reimagine privacy in this rapidly evolving digital age?
- How can institutions leverage new sources of data and emerging technologies to benefit both customers and service providers without running afoul of privacy regulations or offending consumer sensibilities?
- How should companies go beyond compliance to make privacy management a competitive differentiator?

We discuss these questions and other challenges in detail in this report.

A new framework to understand privacy today

The industry will likely need a more robust, expansive, pragmatic, and forward-looking framework to successfully navigate the evolving privacy landscape. This framework should be

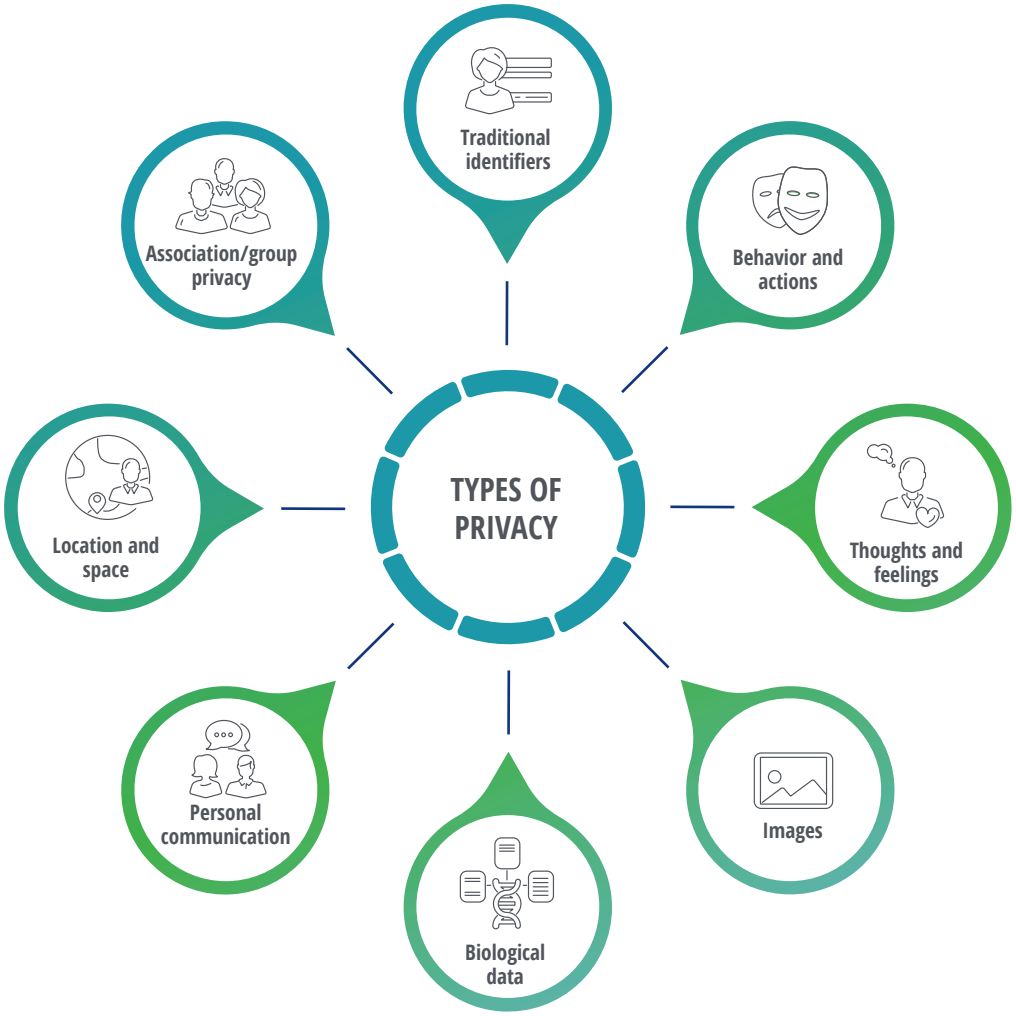
both tactical and strategic—one that would stand the test of time and continue to adapt to future technological innovations.[17]

The framework below was inspired by the work of three researchers—Rachel L. Finn, David Wright, and Michael Friedewald—who identified seven different types of privacy—ranging from *privacy of location* to *privacy of association*. For this report, we modified and expanded their typology to encompass relevant privacy issues the financial services industry currently faces (figure 1). Figure 2 offers more detailed explanations of these eight types.

These eight categories highlight the multidimensionality of privacy today. They underscore the importance for financial services leaders to think differently, and more expansively, about how their organizations collect, store, process, share, and protect information.

FIGURE 1

The eight types of privacy



Source: Deloitte's modified eight types of privacy is based on the work of Rachel R. Finn, David Wright, and Michael Friedewald, "Seven types of privacy" in Serge Gutwirth, Ronald Leenes, Paul de Hert, and Yves Poullet (eds), *European Data Protection: Coming of Age* (Dordrecht: Springer, 2013). The authors posited seven types of privacy, but we modified their framework to make it more relevant for financial services by altering "data and images" to images only, and splitting "privacy of the person" to "traditional identifiers" and "biological data."

Take, for example, the use of biometric data, like facial-, voice-, and iris-recognition for identification in financial services.[18] Data from these technologies could be combined with other personal information, such as location or social media posts, to decipher an individual's needs and preferences for financial services. In a privacy context, what are the expectations regarding the use of such data? Do consumers need to be informed that the merging of private information sources is happening, and how this combined profile may be used to serve them?

Such examination would not be possible without a richer, more nuanced understanding of privacy for today's digital world.

FIGURE 2

Understanding the eight types of privacy

Traditional identifiers	Any standard/traditional personally identifiable information, including demographic data—such as name, address, date of birth, race, gender, and Social Security number—that the industry has routinely collected.
Behavior and actions	Behaviors undertaken in public, semipublic, or private spaces—such as shopping, financial transactions, purchasing financial products, browsing habits, and other behaviors outside the financial relationship.
Thoughts and feelings	Customers' opinions on a variety of topics, including those expressed about companies or brands; also known as *psychographics* in marketing.
Images	Images taken by individuals, planes/drones, satellites, and robotic devices in private or public spaces.
Biological data	Bodily functions and characteristics, including physical characteristics (such as facial features, irides, voice, and gait), physical and psychological health, and genetic code.
Personal communication	Communications between the customer and the financial institution and other entities—via email, text messages, social media, and phone—as well as Web browsing behavior via cookies.
Location and space	Information about a person's or property's geographic location.
Association/ group privacy	Groups and subgroups the customer belongs to or associates with, including political affiliations, personal hobbies, work-related groups, and religious groups.

Source: Deloitte Center for Financial Services.

Privacy implications of emerging technologies

New data sources should be leveraged with caution

Over the next few years, financial institutions are expected to increasingly use evolving technologies to serve their customers, tapping into virtual assistants, personal and commercial sensors, and drones, in addition to already commonplace activities, such as reviewing Web browsing and social media activity.

A major challenge for companies is how to optimize the use of all the data generated by legacy and emerging technologies while remaining within the bounds of privacy regulations.

In many cases, customers are aware that their private data is being collected—for example, when vehicle owners agree to allow insurers to monitor their driving telematically in exchange for discounted auto insurance premiums. But other types of direct data collection and how such information is used might not be as obvious to consumers. This is partly because standard privacy policies usually employ legalistic language and do not offer many details, such as whether companies will use cookies to track Web browsing or check social media for behavioral proclivities when assessing a customer's credit risk.[19]

Would investment management clients be okay if their advisory firm scanned their social media postings, geolocation information, or Web browsing history to determine their interest in socially responsible investments, based on data collected about their charity work or an appearance at a rally protesting fossil fuels? Would they feel uncomfortable if their investment advisor knew they browsed astrological websites before making financial decisions? Would credit card customers mind if their banks checked smart wallet spending patterns to detect if they are often at casinos or the racetrack?

Additional privacy concerns might arise if a financial services firm sells customer data to third parties—personal health data from a wearable monitor, for instance. In such cases, consumers may not be aware of the extent of data mining for it to qualify as "informed consent."

Also, as noted earlier, we might see more cases of consumers and privacy advocates insisting on the "right to be forgotten," codified under GDPR, where consumers may ask data companies to remove certain digital bread crumbs from their online history. Consumers may opt in, however, if they are presented with a value proposition that makes it worth their while to share such data.

More generally, though, a major challenge for companies is how to optimize the use of all the data generated by legacy and emerging technologies while remaining within the bounds of privacy regulations. Financial institutions cannot focus on compliance alone. Even if they meet all legal requirements, they need to ensure their data mining

from a growing number of sources does not alienate consumers or lawmakers.

Technologies' impact on privacy will vary

We analyzed eight tools and technologies that either already are, or will likely become, ubiquitous to determine how likely they are to encroach on privacy. (Please see the sidebar "About our research" on page 8 for our assessment methodology.)

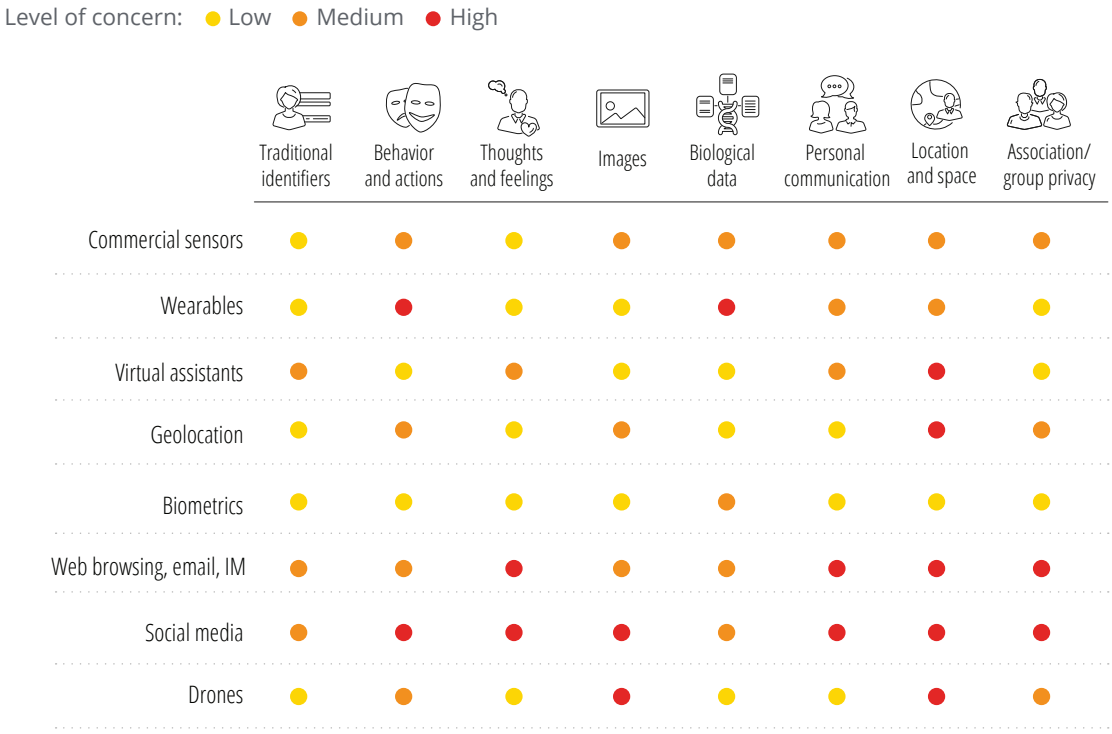
While no area appears to be completely immune from a potential privacy concern (see figure 3), the threat level varies considerably according to the type of tool or technology employed.

Our analysis suggests some technologies are more likely to create privacy concerns than others. Monitoring of Web browsing and social media are most likely to raise objections. Commercial sensors, wearables, virtual assistants, and drones are others with substantial potential for encroachment. Biometrics is probably the technology with the lowest potential to invade privacy.

But in looking at the types of privacy, the greatest causes for concern at this point in time are *location and space*, *communications*, *thoughts and feelings*, and *association and group*. Monitoring of *behavior and actions* could also be a challenge based on our assessment.

FIGURE 3

Potential of technology/tool to encroach on individual privacy, by type of privacy



Source: Deloitte Center for Financial Services.

ABOUT OUR RESEARCH

In assessing the potential of each technology or tool to raise privacy concerns, we considered three factors: 1. How easy is it to collect consumer data; 2. How prevalent it is in society; and 3. How widely it is used in financial services.

For each type of privacy, we assigned a value between 0 and 2 for each of these factors, with "0" being nonexistent or low; "1" being somewhat; and "2" being high. The scores were then summed up across the three factors, with equal weighting, to arrive at a final score for each technology by type of privacy.

The possible range of this total score is 0 and 6. If the total score was 0 or 1, we termed the potential threat level as *low*; if it was 2, 3, or 4, we deemed it *medium*; and if 5 or 6, we considered it *high*.

It's important to note that our analysis is only about the current state of existing technologies. It is quite possible that there could be other tools developed over the next few years that might have more significant implications for personal privacy. In addition, existing tools may be used more widely by financial services firms in the future to gather customer data, and thus become more intrusive on privacy.

Privacy is all about the context

Beyond how personal data is collected, concerns about privacy are often more about the context—why, who, when, and where. For example, companies should be sensitive to what many refer to as the "creepiness factor," where customers might find the way companies gather data about them is too intrusive, such as creating a profile based on an individual's online activity or marketing to them accordingly.[20] Companies need to be cognizant of where to draw the line and clearly communicate to consumers where that line is in their privacy policies.

So, how can financial services leaders determine where that line should be? Here are a few scenarios to think about: A drone might be used to assess the condition of a property for mortgage or investment purposes, or during an insurance claim investigation, but it could also be deployed to surreptitiously determine someone's location or record what the person is doing (behaviors and actions) at a particular time and place. Similarly, geolocation technology or Web browsing (how you press, scroll, and type on a phone screen or keyboard) can be used to detect actions like fraud,[21] but also for other potentially invasive purposes, such as tracking one's location patterns and online habits.

Wearables, another rich source of customer data, are already used by life insurers to motivate policyholders to stay fit in return for lower premiums,[22] and by banks for identity authentication or to enable seamless payments.[23] But companies could also use data from wearables to see if a customer is spending more time at fast food restaurants than at the gym, which some might consider too intrusive. Gait analysis is another way to authenticate identity and mitigate against fraud but could also be used to make inferences about a person's health, which could be a line-crosser for consumers.

Even more controversial is how data from different emerging technologies could be combined to make even more precise assessments about customers. Biometric data from facial recognition software, for example, could be cross-referenced with social media posts to identify a loan applicant's risk profile. While privacy policies may imply that a wide variety of tools and technologies are being utilized to gather data, few, if any, explain why or how multiple sources might be correlated as part of a broader data analysis, or the potential implications of doing so.

Most times, however, financial institutions would not have to go to extremes to gather the data they need to make a decision about a consumer. Consider how monitoring social media posts could red flag an applicant who posts pictures from a

recent skydiving adventure or trapeze lessons. These could be potentially valuable data points for a lender, insurer, or even an investment management firm, as thrill seekers may also be less risk-averse in their investment choices, or, on the other hand, be too risky for a life insurer to cover.

New York regulators recently gave life insurers the green light to use social media posts as well as other nontraditional data sources to help determine premium charges, provided insurers can prove such data doesn't unfairly discriminate based on race, gender, color, or sexual orientation.[24] Most consumers may not be aware that such intimate, yet easily available information could be accessed by their financial services provider.

However, if consumers are made aware—not just about how their social media postings are used, but about the potential value such monitoring might provide for them—it could make a big difference. In a Deloitte survey conducted in 2016, only 15 percent of consumers were willing to share their Web browsing activity and only 12 percent their social media postings with service providers.[25] But if financial institutions fully disclose the source of the data and the reason for collecting it, and clearly communicate the value equation, privacy concerns perhaps could be overcome.

Indeed, another study found about two-thirds of 18- to 34-year-old respondents, and nearly one-half of 35- to 54-year-olds would be willing to allow insurers to sift through data from social media, smart homes, or even health monitoring devices if it could lower their premiums.[26] But what if such monitoring resulted in higher premiums? What would happen to the value equation then? This is something both institutions and consumers should consider.

Meanwhile, despite the growing popularity and the expansive nature of nontraditional customer data, one should also question whether these sources actually provide differentiated insights. "Not all Internet of Things (IoT)-generated data will be useful, and so companies will likely need to gain experience with some of these new data types … in order to discern which are predictive in nature, and update their analytical models accordingly," according to a Deloitte report on the potential opportunities and pitfalls of IoT technology in financial services.[27] One example is usage-based insurance, where it is unclear whether such experiential driving data produces significantly better underwriting and pricing outcomes than using traditional identifiers as proxy factors, such as credit score or age.

Only 15 percent of consumers were willing to share their Web browsing activity and only 12 percent their social media postings with service providers.

Still, generally speaking, consumers may have fewer qualms about the use of data by their financial service providers if there is some meaningful value offered in return. Financial institutions could try to win over consumers by applying a portfolio approach to privacy, showing various scenarios that spell out the possible return customers may receive from sharing various types of data versus the level of risks involved.

Take accelerated life insurance underwriting, where applicants can buy coverage without having to go through intrusive medical exams.[28] Insurers typically conduct a pre-check by accessing data from medical information bureaus, prescription databases, and even motor vehicle records. They can approve a policy if they are satisfied with what they find but cannot reject a candidate based on third-party data alone. At worst, the carrier can request a full medical workup if they need more information before deciding whether to insure a person, and if so, at what price. Disclosure and transparency prevail, with a clear value proposition for both provider and buyer.

But what happens if consumers don't want financial institutions intruding into their personal

lives, whatever digital bread crumbs they've left in their wake? Might they be penalized in some way by opting out of the connected economy? For example, might usage-based auto insurance expand to the point where consumers who refuse to have their driving monitored in real time are automatically surcharged because insurers cannot assess how safely they drive? How might consumers, and regulators, react to that scenario down the road?

Financial services firms that lack the appropriate strategies, policies, and controls to deal with these new forms of data and respond to such provocative questions could be at risk.

PREDICTABLY INACCURATE: THE NEED FOR DATA GOVERNANCE

One of the potential pitfalls of collecting so-called "big data," particularly when provided by third parties (for example, data brokers, consumer reporting agencies, noncommercial aggregators, industry bureaus, and industry/sector-specific data warehouses), is the risk of micro-targeting prospects or basing decisions about customers on information that turns out to be outdated or inaccurate. A recent study by Deloitte found significant inaccuracies in data supplied by a leading consumer information broker, with errors ranging from 10 percent to 50 percent or more on a wide variety of points—including household income, net worth, purchasing behavior, homeownership, vehicles driven, and number of children.[29]

The Deloitte report warns that "perils ranging from minor embarrassments to complete customer alienation may await businesses that increasingly depend on big data to guide business decisions and pursue microsegmentation and microtargeting marketing strategies."[30]

Indeed, according to the report, basing a personalized message or decision about a customer "around wrong or inappropriate information … may not only diminish the effect of marketing efforts, but do more damage than good … causing a customer to move from a neutral, nonexistent, or positive attitude toward the company to a negative one."[31]

Such errors can have grave implications for consumers and institutions alike. What if inverted digits on an entry about blood pressure indicate hypertension when, in fact, the individual has no such health issue? What if a doctor inadvertently hits "select all" on a list of medications when they meant to hit 'unselect all'? Such innocent mistakes, if left uncorrected, could create havoc for individuals whose data is harvested by companies or third parties.

Clearly, more attention needs to be paid to data governance, from acquisition, to confirmation, to correlation of various data and information sources. To minimize this risk, financial institutions should consider more proactive vetting of both their own data and whatever data they receive from third-party vendors. This should include a demand for transparency in an outside firm's data collection, data lineage, validation, refresh timing, and correction methods, among a number of additional due diligence steps.[32] Financial firms should also consider regularly fact-checking their own data and that of outside providers with customers themselves. This practice of reaching out directly could not only help improve accuracy but would show good faith to consumers that financial institutions put a premium on getting their data right.

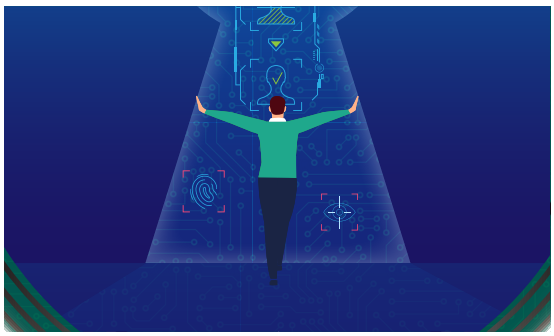
Are existing policies suitable for protecting privacy in the digital age?

Current state of privacy policies in financial services

In the next section, we look at how well financial services firms may be currently set up to address the privacy challenges posed by emerging technologies and nontraditional data. We analyzed privacy policies from a random sample of 12 large financial institutions in banking, investment management, insurance, and real estate to determine what data is collected, how it is stored, shared, and protected, and how frequently privacy policies are updated.

WHAT DATA IS COLLECTED?

Universally, all companies in the sample collect traditional identifiers including (but not limited to) name, email, address, phone number, and Social Security number. Data collected by insurance firms, particularly, was most extensive, given the nature of their work and how data is used for risk selection and to make policy pricing and coverage determinations. In addition to personally identifiable information (PII), insurers in the sample also collected more personal data such as medical or driving history, depending on the line of business. All of those sampled also tracked website analytics data, including browser type, IP address, and app usage.



HOW IS DATA COLLECTED?

The institutions we analyzed assert that their primary data collection method is via "voluntarily supplied or disclosed" consumer data—for example, data that consumers manually enter when opening an online account or applying for a loan or insurance policy. Every company analyzed also uses cookies and Web beacons to collect and track Web data. Some also collect data from third-party resources, such as data brokers.

HOW IS DATA USED?

Every financial institution included in our analysis asserts that its use of consumer data is essential to everyday business purposes and operations, and most emphasized that the manner in which they use data is permissible under law. Most also note that data is used to deliver quality services, such as account management, fraud prevention, and marketing.

IS DATA SHARED AND CAN CUSTOMERS OPT OUT?

Across the board, all of those sampled share data in some way. The majority stipulate that data is shared within the family of companies and subsidiaries, or across business units to "enhance services."

They disclose that data may be shared with third-party providers as required or permitted by law. Furthermore, for the most part, consumers cannot opt out of this data sharing except when it is used for marketing or advertising purposes.

HOW IS DATA PROTECTED?

Most companies state that they "maintain physical, electronic, and procedural safeguards" in line with industry standards.

ARE CUSTOMERS NOTIFIED OF POLICY CHANGES?

As required by law, insurers send consumers an updated privacy policy annually. The rest of the companies note that they reserve the right to modify their privacy policies at will. Some notify consumers of changes, while others advise consumers to regularly refer to their websites for policy updates.

HOW FREQUENTLY ARE POLICIES UPDATED?

Most of the privacy policies examined had been updated within the prior year. One company—an insurer—had not updated its online privacy policy since 2013.

HAVE FINANCIAL INSTITUTIONS GONE FAR ENOUGH WITH PRIVACY DISCLOSURES?

Which of the eight elements of privacy outlined in the framework earlier are mentioned in the policies of the sample companies? We performed a second text analysis on their privacy policies to identify which metrics were tracked as they related to the types of privacy described on page 5 (figure 2).

At first glance, the results looked promising. However, none of the sampled companies accounted for all eight types of privacy, and how they were referenced was arguably superficial. Here's why:

- First, the policies suggest privacy operates on a binary level—whether the company is compliant or not with existing laws—and fail to address the complexities of privacy that have emerged thanks to the latest technological advances.

- Second, none of the policies explicitly mention all the technologies included in our analysis.

- Finally, none of the policies go beyond high-level detail on how or why data is collected and shared, let alone what the potential benefits might be for consumers.

In fact, we found that privacy policies within financial services sectors—banking, insurance, and investment management—were so alike that it was hard to differentiate between firms. This also suggests that current privacy policies are merely "checking the box" to satisfy compliance requirements.

Within the banking segment, for instance, all banks in the sample provided identical, boilerplate factsheets on what, how, and why data is shared. In addition, excluding two investment management firms in the sample that regularly review and adjust their safeguards, most privacy policies are not forward-looking and do not take advances in technology and new data into consideration—a missed opportunity.

As technology continues to advance and new forms of data emerge, how should financial institutions adapt their privacy practices? While traditional forms of consumer data are covered under current financial privacy laws, data from the fusion of new technologies is not. Given the absence of a comprehensive, forward-looking US federal standard, there appears to be a widening chasm of data that financial institution policies do not account for and, most importantly, that companies may not be compelled to account for. Thus, the current state of existing privacy policies may be giving consumers a false sense of comfort, which could be setting the stage for a rude awakening and, subsequently, the potential for a privacy backlash among consumers.

Looking forward: A new way to manage customer privacy

IN THIS REPORT, we propose that financial institutions should rethink customer privacy in a more expansive, proactive, and strategic manner. In short, firms should consider the following:

- **Broaden their lens.** Go beyond superficial checkpoints to account for multiple types of privacy and the tools and technologies capable of encroachment. As a first step, financial institutions should become more proactive and deliberate, exploring how emerging data sources and privacy concerns will likely evolve over time in terms of consumer attitudes, technological innovation, and regulatory constraints.

- **Review and revamp current privacy policies.** Today's policies often include simple disclosure statements to clear regulatory hurdles. Instead, companies should use these policies to earn customer trust by providing enough transparency to demonstrate good faith. Furthermore, institutions could help ease any lingering misgivings about privacy by showing consumers how they could also benefit from the various types of data collection and analysis and including these details in their policies.

- **Be good stewards of the data they collect and purchase.** Companies could improve the quality control, accuracy, and relevance of the data they collect by establishing a more comprehensive privacy governance framework. This would include systematic vetting of data collected in-house and from third parties.

- **Explore new data science techniques to protect sensitive information.** As an example, institutions could add random noise or create synthetic data sets to protect consumers' personal or sensitive information.[33]

- **Make positive use of emerging technologies and new data sources.** Financial institutions should look for ways data can mutually benefit providers *and* consumers. Customers should be kept in the loop as companies explore new data sources and analytical methods, and institutions should openly disclose and explain the proposed value proposition to consumers.

Financial institutions should become more proactive and deliberate, exploring how emerging data sources and privacy concerns will likely evolve over time.

- **Finally, chief privacy officers should be empowered** to develop new privacy management strategies. If such positions don't exist, it might behoove the institutions to appoint someone to lead privacy management.

When all is said and done, financial institutions should be able to meet basic regulatory requirements while also honoring consumer sensibilities about the sanctity of their personal information. Such sensibilities are likely to evolve over time and they could differ across segments and various types of privacy.

Rather than assuming that customer perceptions of privacy are immutable and not susceptible to persuasion, financial services firms can shape how customers view the value of their data. They can engender trust by clearly communicating what they're doing with consumer data and by giving something in exchange, such as tailored offerings, new services, better pricing, or reduced time for service delivery.

These steps can help financial institutions get ready for a future marked by ongoing, rapid technological innovation. Armed with this new, more strategic approach, financial institutions should be better prepared to effectively manage privacy in an increasingly digital world, to differentiate themselves, and, most importantly, to more effectively serve their customers.

Appendix: Recent developments in regulating privacy

THE MOST NOTABLE development in regulating consumer privacy is arguably the adoption of the GDPR in the European Union, which took effect in May 2018. This sweeping regulation impacts every business that handles the personal data of EU citizens, including financial institutions. GDPR protects the personal data of all EU residents, while stipulating that companies must notify EU citizens of data breaches and obtain express opt-in consent to their data, or risk paying steep fines. Consumers also have a "right to be forgotten," and companies are required to erase all personal data currently maintained upon request or if the data no longer serves the original business purpose.[34]

In the United States, regulations tend to be narrower in scope and generally only protect specific types of data or tend to be sector- or industry-specific. The Federal Trade Commission (FTC), an independent legal authority, is tasked with enforcing a number of these laws, including those that regulate consumer privacy as it relates to children, telemarketing practices, consumer fraud, debt collection, and unfair credit and lending practices, to name a few.[35]

As of early 2019, no single, comprehensive federal privacy standard that protects all types of consumer data is in effect in the United States, placing the onus on states to craft their own mandates. California, leading the charge, passed the Consumer Privacy Act in the summer of 2018. Similar to GDPR, it grants consumers sweeping control of all forms of their personal data,[36] from addresses and phone numbers to "likes" on social media or interactions with personal assistants. California's new law is set to take effect in 2020, and although it only applies to California residents, many companies that operate nationally are expected to amend their privacy policies to avoid conflicting standards for consumers in other states.[37] A bill has been introduced in California—AB981—designed to eliminate overlap between the new California law and 1980's Insurance Information and Privacy Protection Act, but consumer groups are lobbying against any carveout for insurers.[38]

Outside California, a number of other state privacy laws exist, but the laws are not as all-encompassing as is California's. Vermont, for instance, enacted a data broker privacy law in 2018, which aims to protect consumers from third-party data brokers that harvest and sell their information without their consent.[39] Delaware, meanwhile, enacted the Delaware Online Privacy and Protection Act in 2016, which requires all firms that collect PII to post privacy policies.[40]

Financial privacy laws

Despite the lack of a single, all-encompassing federal standard, a robust set of regulations governs the US financial services sector. One major law is the Gramm-Leach-Bliley Act (GLBA), which regulates how financial institutions (including banks, securities, and insurance entities) handle and protect nonpublic consumer PII. The GLBA mandates, under its "Financial Privacy Rule," that financial institutions provide notice of their privacy policies and limit their disclosure of PII to affiliated and nonaffiliated third parties.[41] Companies are also required to give consumers notice and a "reasonable opportunity" to opt out of the sharing of some types of data with third parties. Financial firms must

also provide and maintain safeguards to protect consumer PII under another provision of the GLBA known as the "Safeguards Rule."[42]

The Consumer Financial Protection Bureau (CFPB) was given rulemaking authority to enforce much of the GLBA under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank).[43] The FTC also enforces provisions within the GLBA.[44]

Additional financial privacy laws include the Fair Credit Reporting Act (which regulates personal data held by consumer reporting agencies),[45] the Bank Secrecy Act (which compels companies to assist the government in money laundering prevention and detection by sharing consumer activity reports),[46] and the Right to Financial Privacy Act (which grants financial consumers a degree of privacy from the government).[47]

Despite the plethora of privacy rules, public awareness remains limited. A survey of 6,000 individuals in six countries, including the United States, found that more than one-half were unfamiliar with privacy regulations concerning their personal data.[48]

Endnotes

1. Electronic Frontier Foundation, "Privacy," accessed March 4, 2019.
2. Lee Rainie, "Americans' complicated feelings about social media in an era of privacy concerns," Pew Research Center, March 27, 2018.
3. EUGDPR, "The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years," accessed March 5, 2019.
4. Alexandra Bruell, "Advertisers' top trade group pushes for Federal Data Privacy Regulation," *Wall Street Journal*, December 19, 2018.
5. Internet Association, "Internet Association proposes privacy principles for a modern national regulatory framework," press release, September 12, 2018.
6. U.S. Chamber of Commerce, "U.S. Chamber privacy principles," accessed April 8, 2019.
7. Californians for Consumer Privacy, "What does the California Consumer Privacy Act do?," accessed April 22, 2019.
8. Bryan Cave Leighton Paisner, "The top three privacy takeaways of the New Delaware Online Privacy and Protection Act," August 3, 2016.
9. Harry Valetk, Brandon Moseberry, and Bernard L. Hengesbaugh, "Vermont enacts first US Data Broker Privacy Law," Lexology, August 3, 2018.
10. Deloitte Canada, "Privacy for sale: To the highest bidder," accessed April 8, 2019.
11. Will Thomas DeVries, "Protecting privacy in the digital age," *Berkeley Technology Law Journal* 18, no. 1 (2003): pp. 283–311.
12. Daniel J. Solove, "A taxonomy of privacy," *University of Pennsylvania Law Review* 154, no. 3 (2006).
13. William M. Beaney, "The Right to Privacy and American Law," accessed April 8, 2019.
14. Deirdre K. Mulligan, Colin Koopman, and Nick Doty, "Privacy is an essentially contested concept: A multidimensional analytic for mapping privacy," The Royal Society Publishing, December 28, 2016.
15. Carissa Véliz, "What if banks were the main protectors of customers' private data?" *Harvard Business Review*, November 20, 2018.
16. World Economic Forum, "World Economic Forum annual meeting," accessed April 8, 2019.
17. Val Srinivas, "Privacy in the post-GDPR world: How should banks and other financial institutions rethink customer privacy and make it a differentiator?," QuickLook blog, Deloitte Center for Financial Services, March 14, 2018.
18. Matt Burgess, "Your next bank card will have a fingerprint scanner built-in," *Wired*, May 2, 2018.
19. Scram Software, "Does my internet activity affect my insurance and credit ratings," March 18, 2015.
20. Knowledge@Wharton, "Privacy on the Web: Is It a losing battle?," June 25, 2008.
21. Tanaya Macheel, "Are you really there? U.S. bank tries geolocation to stop fraud," *American Banker*, October 17, 2016; Stacy Cowley, "Banks and retailers are tracking how you type, swipe and tap," *New York Times*, August 13, 2018.
22. Lisa F. Carver, "Why Life Insurance companies want your Fitbit data," Medical Xpress, September 24, 2018.

23. Avin Arumugam, "Paying with wearables: The next big thing in IoT," Visa, accessed February 28, 2019.
24. Jessica Baron, "Life Insurers can use social media posts to determine premiums, as long as they don't discriminate," *Forbes*, February 4, 2019.
25. Gina Pingitore et al., *To share or not to share: What consumers really think about sharing their personal information*, Deloitte University Press, September 5, 2017.
26. Tim Sandle, "Are you happy with digital spying for reduced insurance prices?" *Digital Journal*, June 21, 2018.
27. Jim Eckenrode, *The derivative effect: How financial services can make IoT technology pay off*, Deloitte University Press, October 13, 2015.
28. Greg Lacurci, "Technology is streamlining the process of issuing life insurance policies," InvestmentNews, January 10, 2018.
29. John Lucker, Susan K. Hogan, and Trevor Bischoff, "Predictably inaccurate: The prevalence and perils of bad big data," *Deloitte Review* 21, July 31, 2017.
30. Ibid.
31. Ibid.
32. Ibid.
33. Sachin Gupta and Matthew Schneider, "Protecting customers' privacy requires more than anonymizing their data," *Harvard Business Review*, June 1, 2018.
34. EUGDPR, "The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years," accessed April 22, 2019.
35. Federal Trade Commission, *Privacy and data security update: 2016*, 2016.
36. Californians for Consumer Privacy, "What does the California Consumer Privacy Act do?."
37. Marc Vartabedian, "California passes sweeping data-privacy bill," *Wall Street Journal*, June 29, 2018.
38. Timothy Darragh, "California lawmaker, APCI defend insurance privacy bill," BestWire, April 4, 2019.
39. Valetk, Moseberry, and Hengesbaugh, "Vermont enacts first US Data Broker Privacy Law."
40. Paisner, "The top three privacy takeaways of the New Delaware Online Privacy and Protection Act."
41. FDIC Consumer Compliance Examination Manual, "Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information)," June 2016.
42. Federal Trade Commission, "Financial privacy," accessed April 5, 2019.
43. FDIC Consumer Compliance Examination Manual, "Gramm-Leach-Bliley Act."
44. Federal Trade Commission, "Financial privacy."
45. Federal Trade Commission, "A summary of your rights under the Fair Credit Reporting Act," accessed March 5, 2019.
46. Federal Deposit Insurance Corporation, "Bank Secrecy Act, Anti-Money Laundering and Office of Foreign Assets Control," accessed March 5, 2019.
47. FDIC Consumer Compliance Examination Manual, "Gramm-Leach-Bliley Act."
48. Deloitte Canada, "Privacy for sale."

About the authors

VAL SRINIVAS is the banking and capital markets research leader at the Deloitte Center for Financial Services. In his role, Srinivas works closely with the center and extended Financial Services team to support and continue the development of our thought leadership initiatives in the industry, coordinating our various research efforts and helping to differentiate Deloitte more effectively in the marketplace. Srinivas has more than 15 years of experience in research and marketing strategy. He is based in New York.

SAM FRIEDMAN is the insurance research leader at the Deloitte Center for Financial Services, where he analyzes the latest trends and identifies major challenges confronting the property-casualty, life insurance, and annuity industries. Friedman joined Deloitte in October 2010 after 29 years at National Underwriter P&C, where he was editor-in-chief. He has written several articles for Deloitte Insights, including reports on cyber risk management in financial services and obstacles to cyber insurance development. He is based in New York.

TIFFANY RAMSAY is a senior market insights analyst at the Deloitte Center for Financial Services, Deloitte Services LP, where she contributes to research initiatives that differentiate the center as a thought leader in the financial services industry. She has more than five years of experience in research. Ramsay holds a bachelor's degree in sociology and a master's degree in public administration from Cornell University. She is based in New York.

Acknowledgments

The authors wish to thank the following Deloitte client service professionals for their contributions to this article:

Michelle Chodosh, senior manager, Deloitte Services LP

Patricia Danielecki, senior manager, Deloitte Services LP

Chris Faile, senior manager, Deloitte Services LP

Erin Loucks, manager, Deloitte Services LP

Omer Sohail, principal, Deloitte Consulting LP

About the Deloitte Center for Financial Services

The Deloitte Center for Financial Services, which supports the organization's US Financial Services practice, provides insight and research to assist senior-level decision-makers within banks, capital markets firms, investment managers, insurance carriers, and real estate organizations. The center is staffed by a group of professionals with a wide array of in-depth industry experiences as well as cutting-edge research and analytical skills. Through our research, roundtables, and other forms of engagement, we seek to be a trusted source for relevant, timely, and reliable insights. Read recent publications and learn more about the center on Deloitte.com.

Contacts

INDUSTRY LEADERSHIP
Kenny Smith
Principal
US Financial Services leader
Deloitte Consulting LLP
+1 415 783 6148
kesmith@deloitte.com

EXECUTIVE SPONSOR
John Lucker
Principal
Deloitte and Touche LLP
+1 860 725 3022
jlucker@deloitte.com

DELOITTE CENTER FOR FINANCIAL SERVICES
Jim Eckenrode
Managing director
Deloitte Center for Financial Services
Deloitte Services LP
+1 617 585 4877
jeckenrode@deloitte.com

Val Srinivas, PhD
Banking and capital markets research leader
Deloitte Center for Financial Services
Deloitte Services LP
+1 212 436 3384
vsrinivas@deloitte.com

Sam Friedman
Insurance research leader
Deloitte Center for Financial Services
Deloitte Services LP
+1 212 436 5521
samfriedman@deloitte.com

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Karen Edelman, Blythe Hurley, Nairita Gangopadhyay, and Abrar Khan

Creative: Emily Moreano

Promotion: Ankana Chakraborty

Cover artwork: Emily Moreano

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

About Deloitte