The New Privacy: It’s All About Context
by Fatemeh Khatibloo, December 19, 2013

KEY TAKEAWAYS

Companies Must Practice Contextual Privacy
Contextual privacy is a business practice in which the collection and use of personal data is consensual, within a mutually agreed upon context, for a mutually agreed upon purpose.

Contextual Privacy Can Be A Business Differentiator
Companies that embrace contextual privacy can differentiate based on treating their customers with more respect. Those that don’t risk regulatory and publicity problems and consumer-driven backlash.

Better Practices Today Include Transparency, Choice, And Caution
Practice a discipline of “no surprises” with your data. Enable customers to make informed choices about the data you collect. Collect only the data that you need and store it no longer than you need it.
The New Privacy: It’s All About Context

Adopt Contextual Privacy To Gain A Market Advantage

by Fatemeh Khatibloo

with Josh Bernoff, Eve Maler, Sarah Rotman Epps, Elizabeth Ryckewaert, and Wilton Arellano

WHY READ THIS REPORT

“Privacy is dead”: It’s a trope so often repeated you might actually think it’s true. But in the age of smartphones and sensors, privacy is not only possible, it’s essential for building trust, the foundational currency of social, mobile, and local services. Context is key: Businesses crave insight into the context in which consumers are using their products, and consumers want businesses to deliver contextually relevant services. Contextual privacy is a framework for negotiating the collection and use of personal data that ensures a fair value exchange for both the customer and the business. This report will explain what contextual privacy is, why you must adopt it, the best practices we see today, and the ones we expect to see tomorrow.

Table Of Contents

2 Privacy Isn't Dead, Though We Understand Why You Might Think It Is
3 Two Reasons You Must Do Privacy Better
6 Privacy's Future Is About Context And Value
11 The Principles Of Contextual Privacy: Transparency, Choice, Caution
17 In The Future, Contextual Privacy Equals Trust And Success

WHAT IT MEANS
18 The Privacy Wars Have Broad Implications

20 Supplemental Material

Notes & Resources

Forrester spoke to 28 vendor and user companies, as well as advocacy groups, industry groups, government representatives, and academics in the fields of privacy and security in preparing this report.

Related Research Documents

Introducing Forrester’s 2013 Data Privacy Heat Map
May 21, 2013

Introducing Adaptive Intelligence
May 8, 2013

Personal Identity Management
September 30, 2011
PRIVACY ISN’T DEAD, THOUGH WE UNDERSTAND WHY YOU MIGHT THINK IT IS

People have been worried about privacy for decades. As long ago as 1970, a Newsweek cover showed a couple cowering under the glare of Uncle Sam, microphones, cameras, and phone taps with the headline “Is Privacy Dead?”¹ In 1999, Scott McNealy, then CEO of Sun Microsystems, told a group of reporters: “You have zero privacy anyway. . . . get over it.”² And in 2010, Mark Zuckerberg argued that consumers’ social norms regarding privacy have “evolved over time,” which justified ongoing changes in Facebook’s approach to privacy.³ So is privacy really dead? It might look that way, especially because:

- **Companies often collect more data than they really need.** TuneIn, a popular streaming radio application for smartphones, doesn't need a user’s birthday or ZIP code to deliver its radio services or even to target relevant ads, but the app requires both of those bits of data, and more, before users can start listening. And, just this year, Google admitted to having needlessly — and illegally — scooped up passwords, emails, and other personal data from open Wi-Fi networks while it was creating its Street View mapping product.⁴ These types of activities are symptoms of a “why not collect it if you can” mentality that is common in online and mobile applications.

- **The data that companies collect extends to intimate, offline moments.** With wearable sleep-tracking devices like the lark, Jawbone UP, and Fitbit Flex, consumers are literally taking their devices to bed with them. In addition, environments that consumers think of as offline, such as retail stores, are increasingly using tracking technologies to improve their understanding of shopper behavior. Security camera footage feeds into software that analyzes shopper demographics, public Wi-Fi networks sniff device data and track in-store foot traffic, and even store shelves are getting “smart,” with facial recognition and mobile device sensors to improve in-store messaging.⁵

- **Voluntary “data stewardship” is unreliable.** Even companies who attempt to practice good privacy and data protection sometimes fail. The social networking app Path, for example, was fined $800,000 by the Federal Trade Commission (FTC) in 2013 for inadvertently downloading users’ address books without permission.⁶ TomTom, maker of global positioning system (GPS) navigation products, felt a backlash when Dutch police used its aggregated map data to optimize speed trap locations. Although the company reacted within hours by changing its licensing terms to disable that use, and proved that it was not sharing individual user data, customers still “felt betrayed.” Neither of these incidents was malicious or even intentional, but they occurred because of an oversight in how particular data was being treated.

- **Governments demand corporate data to augment their security intelligence.** As the National Security Agency (NSA) Prism debacle has made abundantly clear, companies who collect customer data may well be forced to hand that information over to law enforcement agencies under subpoena.⁷ And, increasingly, governments are requiring that corporations turn over data to help improve public health, determine funding of social welfare programs, or improve tax compliance.
TWO REASONS YOU MUST DO PRIVACY BETTER

We don't believe privacy is dead. We do believe that it needs a new definition for a world where smartphones and sensors, social media, and open data are the norm. These new technologies, while tremendously exciting, also present a host of new privacy challenges to both organizations and individuals. Why change your privacy practices? Both to reap opportunity and to avoid disaster.

The Opportunity: Differentiate With Better Privacy Practices

While only a minority of consumers act for change in privacy practices today, we believe there is an opportunity to build significant trust with consumers, irrespective of their age (see Figure 1). If you wait for consumers to get annoyed and ask you to change, you’ve missed the chance to build trust with them proactively. According to Leigh Nakanishi, senior data security and privacy strategist in Edelman’s Technology practice, “We’re seeing privacy as a differentiator more and more; one retail technology vendor we work with wants to put it front and center.” Appropriate privacy practices will be the next business-led, consumer-friendly source of differentiation, similar to what happened in these other industries:

- **Makeup went “cruelty-free.”** In 1988, a small cosmetics company called The Body Shop, based in the UK, started making waves in the US. Its story: products that were never tested on animals (“cruelty-free”) and that never exploited labor or goods from developing countries. By the end of the next decade, The Body Shop had grown to 290 stores in the United States, with revenues in excess of $161 million. The new market category it created — sustainable personal health products — is now worth $117 billion in the US alone.

- **Movies and games adopted rating systems.** When the Motion Picture Association of America proposed an industry-driven series of maturity ratings, it was an attempt to avoid a national censorship board. Not only did studios widely adopt the ratings, they even use it as a marketing ploy, releasing different versions of the same film with different ratings. The rating system has spread to video game manufacturers to provide consumers with more transparency and choice.

- **Music compact discs went eco-friendly.** In the early nineties, when compact discs were the latest hotness, they were packaged in massive, shrink-wrapped cardboard boxes. It didn't take long for environmentalists — including the powerful Sierra Club — to take the recording industry to task over this wasteful packaging. As a result, the six recording companies responsible for 95% of the industry’s sales agreed to do away with the boxes in 1992, replacing them with the now-standard jewel boxes.
Milk eschewed growth hormones. In 1993, after recombinant bovine growth hormone (rBGH) gained US Food and Drug Administration (FDA) approval, a grassroots movement began to take shape against its use in dairy cows. The public outcry was so effective that, by 2000, the European Union, Canada, Australia, New Zealand, Japan, and Israel had banned the hormone’s use, while in the US many dairies and grocery chains made a significant move toward “rBGH-free” dairy products. By 2007, According to Physicians for Social Responsibility, 67 of the top 100 dairies in the US had reduced or eliminated the use of bovine growth hormone.

Figure 1: Consumers Avoid Businesses Whose Privacy Policies They Don’t Like

33% percent of US online adults who read privacy policies have NOT completed an online transaction because of the terms of use or privacy policy

Source: North American Technographics® Media And Advertising Online Benchmark Recontact Survey, 2013

Base: 4,142 US online adults (18+) who read privacy policies

Source: Forrester Research, Inc.
The Risk: Poor Privacy Practices Will Kill Your Business

Maybe you don’t believe you can or should differentiate on the basis of privacy. Or perhaps you think you don’t need to get started right now because, hey, the Internet giants aren’t exactly racing toward the “good privacy” finish line. But unlike Google and Facebook, most firms don’t have a virtual monopoly on their business model. If, like the vast majority of companies, you sell consumer products or services in an increasingly competitive global market, getting privacy wrong poses tremendous risk to your business.\(^{17}\) Over the next few years, companies who don’t have consistent and transparent organizationwide privacy practices in place will suffer:

- **Increased regulation and lawsuits.** In September 2013, California Governor Jerry Brown signed three privacy bills into law that directly affect every company that collects personally identifiable information (PII) from customers in California. These laws extend the definition of personal data, require companies to provide more notice about online tracking, and give minors the right to request that companies delete their personal data.\(^{18}\) The European Union (EU) is also updating its already stringent Data Protection Directive to further restrict the collection and use of data about its citizens, even by companies based outside the EU. These regulations will severely limit US-based companies’ ability to do business globally if they stick with their current inconsistent privacy practices.

- **Publicity nightmares that force organizational changes.** Acxiom, a 40-year-old consumer data giant, was featured prominently in a series of stories by The New York Times, which led to aggressive questioning by the US Congress and Federal Trade Commission (FTC).\(^{19}\) Ultimately, the firm launched a new consumer portal that lets people opt out of its databases or edit the information Acxiom has about them.\(^{20}\) And companies that have chosen to make privacy a business differentiator are now targeting their competitors’ practices. Microsoft’s “Scroogled” campaign forced Google to go on the defensive about its privacy practices and to spend heftily on advertising and public relations to defuse the bad press.

- **Consumer-driven data disintermediation.** Products like AVG Technologies’ PrivacyFix and AdBlock Plus let consumers take control of the data they “leak” as they navigate the Internet. Our consumer surveys show that 25% of online adults are using these tools, while another 19% have turned on the “do not track” setting in their browsers. And 8% have installed “informant” tools like Ghostery that display tracking elements for every site they visit (see Figure 2). As these kinds of tools become even more disruptive and better adopted, today’s “stealthy” online behavioral tracking programs won’t be able to keep up.
PRIVACY’S FUTURE IS ABOUT CONTEXT AND VALUE

What path must companies navigate to differentiate based on privacy and avoid risks? Consumers themselves are giving us the answer. Most tell us that they are willing to share their personal data if it provides value that they are interested in (see Figure 3). But they also want to be able to opt out, limit collection at certain times, and ensure their data isn’t retained forever. And they want to see tangible benefits to the collection and use of their information. In other words, the new privacy is all about context. Forrester defines contextual privacy as:

A business practice in which the collection and use of personal data is consensual, within a mutually agreed upon context, for a mutually agreed upon purpose.

The calculus of contextual privacy is simple: 1) consumers must get commensurate value in exchange for their data, and 2) businesses can recognize new business opportunities when they put contextual privacy to work. As the director of insights at a major investment firm told us, “Our brand means integrity; privacy, and how we treat data, has to be part of our brand message.”
**Privacy Practices Must Respect Five Contexts**

To attain the benefits of better privacy practices and avoid the risks of worse ones, companies must practice contextual privacy by allowing their customers to dynamically negotiate the collection and use of their personal data. An airline app, for example, might provide benefits to a customer by tracking her location, with permission, when she is in the airport on the day of travel, but not at other times or other locations. We’ve identified five types of contexts that marketers practicing contextual privacy must respect (see Figure 4 and see Figure 5):

- **Temporal context.** This is the “when” of data collection and use. For example, a user might decide to block data collection by ad networks as he plans his wife’s surprise party on a shared home computer. Or a working mother might choose to receive coupons from her local grocer on Wednesday afternoons so they’re at her fingertips — on her mobile device — when she gets to the store.

---

**Figure 3: Consumers Are Willing To Exchange Information For Value**

“Which of the following would motivate you to share your personal information with the companies and service providers you interact with?” (Multiple responses accepted)

- Cash rewards: 41%
- Loyalty program points: 28%
- Exclusive deals/discounts on products and services with that company: 21%
- VIP perks (e.g., reservations, skipping lines): 16%
- Exclusive deals/discounts on products that you identify as being of interest to you: 16%
- Higher quality customer service: 15%
- Easy identification via saved information: 15%
- Entry into sweepstakes or prize drawings: 14%
- Faster customer service: 11%
- Other: 2%
- Nothing would motivate me to share personal information with companies: 42%

Source: North American Technographics® Media And Advertising Online Benchmark Recontact Survey, 2013

Base: 5,012 US online adults (18+)
- **Spatial context.** Location is an increasingly important element of the customer data that firms collect because it lets them tailor services, offers, content, and advertising based on where a customer is. But companies should take a “least knowledge” approach to location: Kia Motors America, for example, needs to know if customers are near the dealership to offer a particular service, but it doesn’t need specific details about their location if they’re not.

- **Functional context.** Consumers use specific tools or services to meet specific needs, so the use of their data must support those needs. For example, consumers often provide their email address for informational purposes, but not for marketing purposes. Functional context is especially important for makers of wearable and other sensor-laden devices. A mother might, for example, enable her teenager’s car to send specific driving habits to her smartphone, but not share that data with her insurance company.

- **Identity context.** We all have multiple identities that we assert in different situations. In Toys R Us, a shopper may wish to be recognized as the mother of two preschool-aged kids, living in a home with a backyard. But that identity might not be relevant when the same person is researching elder care options for an aging parent. Advertisers, especially, must let consumers “assert” the identity that’s most meaningful to the activity they’re undertaking by letting users select the unique phone number, social media profile, or browser settings they want to use for a particular interaction.

- **Social context.** Finally, customers frequently wish to share information like discounts and recommendations with their peers. For example, a traveler might choose to share flight arrival information in her Twitter feed, but share an entire travel itinerary — including the right to make changes to it — with her personal assistant. Brands must provide granular choices for these types of sharing. They should never collect information about the people *with whom* data is shared, unless those people specifically grant permission.
**Figure 4** Contexts: What They Mean and Best Practices For Each

<table>
<thead>
<tr>
<th>Context</th>
<th>What does it mean?</th>
<th>Examples</th>
<th>Best practice</th>
</tr>
</thead>
</table>
| Temporal| When can my company collect and use data about you?                                | • On the day of my service appointment  
• The week before my child’s birthday  
• On Wednesday afternoons                                                                                                                        | Let customers “turn off” behavioral tracking and provide preferences about the best time to communicate with them.                                                                                             |
| Spatial | Where can my company collect and use data about you?                               | • When I’m near your store  
• Only if I turn on GPS  
• When I’m near my health-tracker device                                                                                                           | Minimize location data collection with a “least knowledge” approach; e.g., geofencing is better than GPS; binary (yes/no) is better than analog (where, exactly).                                              |
| Functional| How can my company collect and use data about you?                                | • For marketing offers from you  
• For marketing offers from partners  
• For informational uses only  
• For this interaction only; delete when complete                                                                                               | Provide clear explanation for the use of requested data, options for limiting its use, and information about how long data is retained after its use.                                                              |
| Identity | What identity do you want to use when you interact with my company?                | • I’m a business owner researching competitors.  
• I’m a mom shopping for my family.  
• I’m a personal assistant helping my boss.                                                                                                      | Let customers choose profiles, when possible, to ensure your messaging is in line with their emotional context and need.                                                                                         |
| Social  | Who should my company share your information with?                                 | • Share this information to my Facebook wall.  
• Email this receipt only to my insurance company.  
• Grant access to my family, anytime they ask.                                                                                                  | Provide granular data-sharing controls, and never collect data about the recipient without consent. Provide clear notice about data-sharing practices with third-party partners, and allow customers to opt out. |
Figure 5 Contextual Privacy Use Case: How An Airline's Permission Negotiations Can Work

**Spatial context**
WHERE can we access your location data?
- Near the airport? **YES**
- Anywhere? **NO**

**Temporal context**
WHEN can we access your data?
- On the day of travel? **YES**
- Anytime? **NO**

**Functional context**
HOW can we use your data we collect?
- For flight notifications? **YES**
- For marketing and promotions? **NO**

**Identity context**
WHAT identity can we collect data for?
- Frequent flyer, only? **YES**
- Other identities, e.g., as a mom? **NO**

**Social context**
WHO can we share your data with?
- Alert my assistant of flight status. **YES**
- Share flight to social media? **NO**

**Airline XYZ agrees to:**
- Only access location data when customer is near the airport.
- Only access customer data on the day of travel.
- Only use this data to send notifications regarding a specific flight.
- Only access customer data if customer is on business travel.
- Only share travel data with approved contacts.
THE PRINCIPLES OF CONTEXTUAL PRIVACY: TRANSPARENCY, CHOICE, CAUTION

If the elements of contextual privacy seem impossible to implement, don't despair. While the practice isn't widespread yet, some companies are already adopting approaches that help them differentiate with privacy. To begin practicing contextual privacy, avoid potentially disastrous risks, and earn the kind of trust that consumers will demand in order to share their data in the future, firms must do three things immediately:

- **Practice the doctrine of “no surprises.”** One company with a no-surprises privacy policy is Progressive Casualty Insurance. The insurer’s Snapshot product depends on consumer trust — customers install a sensor device in their car to track driving behavior so that Progressive can provide a risk-adjusted insurance policy quote. Progressive’s general manager of usage-based insurance told us, “We set a very high standard for transparency . . . so we had to create a separate, more restrictive privacy policy for the Snapshot.” That policy states, in plain language, what type of data Progressive collects, how it uses that data, and, importantly, how it won't use that data (see Figure 6).

- **Give consumers choices for participating with your service.** Walt Disney Parks and Resorts gives customers lots of choices as it rolls out its new MagicBand, a radio frequency identification (RFID)-enabled wristband used for identity validation and payment. In a letter to Congressman Ed Markey, Disney chairman and CEO Bob Iger laid out the company’s “privacy by design” approach to its practices (see Figure 7).22 For example, visitors can opt in to have specific characters “recognize” their child as they walk through the park or to synchronize their ride ticket times (via Disney’s FastPass) with dinner reservations and shows they wish to see. And, of course, guests can opt to not use the wristband at all.

- **Treat more data as “personally identifiable.”** Researchers have proved that identity can be reverse engineered from seemingly anonymous data. In one study, just four location reference points (e.g., tweets or Foursquare check-ins) were sufficient.23 In another, researchers found that 87% of people in the US could be identified by combining just three data points: five-digit ZIP code, birth date (including year), and gender.24 So as you collect customer data, think twice about whether it's potentially PII.25 MapMyFitness, for example, normalizes citywide activity data and creates “courses” for common overlapping areas such as park trails and bike routes; the result is that the start and endpoints of users’ tracks are suppressed, which ensures that the service doesn't inadvertently expose where people live and work.
**Figure 6** Progressive’s Snapshot Privacy Policy Meets Many Contextual Privacy Best Practices

**Snapshot® Privacy Statement**

At Progressive, we’re committed to protecting your privacy and earning your trust. We understand that you value your privacy, and that you may have concerns about how we use the data we collect.

**Your Driving Story**

Snapshot is our exclusive program that allows you to get a personalized car insurance rate based on how you drive. While we still take into account traditional factors in providing your quote, and previous accidents or traffic violations, Snapshot also considers your actual driving behavior.

We offer Snapshot because it allows you to tell us your driving story and allows us to give you an accurate insurance quote or rate using the latest technology. Knowing more about your driving helps you to give us your best rate, which is better for our customers, and helps you to control your insurance premium, which is better for you.

**Data We Collect**

The Snapshot device records vehicle speed and time of day, and when the device is connected and disconnected from the vehicle. It also records the Vehicle Identification Number upon installation, and the length of time that the device is installed.

**Data We Don’t Collect**

Snapshot focuses on how safely, how often, how far, and when you drive. It does not contain GPS technology and does not track vehicle location.

**How We Use the Data**

Snapshot data is:

- transactional information used to calculate your Snapshot score, which, along with other traditional rating factors, is used to determine your insurance quote or the rate you will pay when you drive will help you control your insurance quote or rate, respectively.
- encrypted when transmitted from the Snapshot device to our servers. Once in our servers, we limit access to the data and use physical, electronic, and procedural safeguards to help protect the data.

**How We Won’t Use the Data**

- We will not sell personally identifiable Snapshot data to any third parties.
- We will not use Snapshot data to resolve an insurance claim you have with us without first obtaining permission from you or the vehicle owner.

Source: Progressive Casualty Insurance website

Source: Forrester Research, Inc.
Figure 7 Disney’s MagicBand Policy Is Entirely Choice Based

MyMagic+ is a completely optional program

Guests can enjoy admission to the park without having to register or provide any personal information. But guests who do choose to participate in MyMagic+ will enjoy the convenience of having their tickets, guaranteed ride times for shows and attractions, resort room access and other enhanced features all in one place. Using MagicBands or cards for purchases is also optional.

MyMagic+ was designed with privacy controls from the outset

The hallmarks of privacy by design are transparency and customer control, and these are central to Disney’s overall privacy policies and practices, which can be found at http://corporate.disney.go.com/corporate/pp.html

Disney does not use personal information to market to children under age 13
Disney does not personalize or target advertisements to an individual child
Disney never shares children’s personal information with any third party for their marketing purposes
Parents have full control over their child’s participation in MyMagic+

Parents control whether or not their child participates in MyMagic+, how much information is shared with us, what experiences the child will engage in and whether they use a MagicBand at all. Children cannot create individual registration accounts for MyMagic+.

Parents decide whether to provide information about their child's preferences (such as favorite character or favorite color) for personalized services. These personalized services also are optional.

No matter what the parent decides, Disney does not use personal information to market to children under age 13 and does not personalize or target advertising to individual children. Furthermore, we never share children’s personal information with any third party for their marketing purposes.

Source: Politico website

Four Steps Can Bring You Closer To Contextual Privacy Today

There's no doubt about it: Moving your organization from current, traditional privacy practices to contextual privacy will be disruptive. Most of your business processes aren't designed to consider their impact on privacy; your technology and systems won't always support new privacy-led approaches; and no matter how customer-centric your culture, privacy is probably not central to it. But whether driven by risk avoidance, regulation, or the pursuit of differentiation, you're going to need to get there. So here's how to get started with contextual privacy:
- **Create a cross-functional privacy task force with enforcement powers.** The digitization of everything and the ubiquity of personal data will take privacy out of the legal and IT world and into business strategy. Firms should create a cross-functional working group that includes members from marketing, product development, operations, customer experience, legal, and IT. This task force must have the authority to enforce the organization's privacy guidelines, and it should authorize any new uses of customer data.

- **Establish an internal data privacy standard.** Most firms leave the work of privacy to their legal teams or their chief information security officers (CISOs), who often write internal guidelines that are incomprehensible to marketers and business strategists. These documents focus on security and compliance issues like data transfer, storage, and encryption. Instead, the privacy task force should create a plain-language internal data privacy standard that outlines rules around collection, retention, use, and sharing of customer data, both within and outside the organization.

- **Audit all of your data collection, retention, and use practices.** The internal data privacy standard serves another important purpose: It becomes the basis for auditing existing and future practices. This audit is a massive undertaking because most companies’ data still lives in widely disparate silos and is managed by multiple teams. But the audit is a critical aspect of getting contextual privacy right, because it enables companies to write a simplified privacy policy that can stand up to scrutiny by any governing body or customer advocacy group.

- **Simplify your external-facing privacy policies.** While we don't imagine that the multipage privacy policy or terms of use will disappear — they are legally binding agreements, after all — we do suggest that companies take a two-tier approach to their consumer-facing privacy pages. Follow the example of mobile apps and Creative Commons licenses: Provide a simplified set of information outlining your approach to contextual privacy, but let customers drill down to get further information if they wish to (see Figure 8).
Figure 8 Mobile Apps And Creative Commons Are Examples Of Good Two-Tier Information Sharing

This Android mobile app provides at-a-glance descriptions of the data it accesses on your device and the permissions it is granted. Tapping any icon on the main permissions screen (left) gives the user a deeper explanation of that permission, including how it might be used (right).

Source: Creative Commons website

Future Practices To Work Toward: Real-Time Negotiation With Adaptive Intelligence

Every company can practice the basics of transparency, choice, and caution today. Meanwhile, technologies are emerging that will enable companies and people to negotiate, in real-time, how they wish to exchange data.29 Examples of these types of dynamic negotiations include:

- **Mediated trustworthiness.** Firms like TRUSTe, McAfee, and Appthority are already helping companies become more privacy compliant. Privacy software maker Disconnect is working to crowdsource a set of icons that will simplify privacy policies for individuals (see Figure 9). In the future, these firms and others will provide badges or seals that help consumers decide whether to share data with a company, on the fly.
- **Identity credentials and data selected and controlled by the user.** Many companies have already enabled “social sign-in”: The user chooses one of his or her existing online profiles as a single sign-on (SSO) method to access a third-party site. Amazon.com, Facebook, Google, LinkedIn, PayPal, Twitter, and others can function as identity providers (IdPs), and together they cover nearly all online individuals globally. Firms that enable SSO limit risk by outsourcing user login and password reset jobs, without giving up access to permission-based user data. Specialty vendors such as Gigya and Janrain support the full range of IdP options, while many other vendors enable a basic set of IdPs.

- **Preauthorization of data usage for specific contexts.** It's not realistic or ideal to ask customers to negotiate permissions, in real-time, every time they interact with a brand. Instead, we envision preauthorization of data usage for specific contexts. For example, in the airline scenario described earlier, the negotiation of spatial and temporal contexts, which frequently change, could occur when the user first downloads and configures the app to her mobile phone. She wouldn't have to do it for every trip, although she'd have the ability to make changes anytime.

- **Just-in-time data access, instead of data collection.** As the tools and technologies for personal identity and data management (PIDM) improve, organizations won't need to capture and store every last piece of data about their customers. Instead, they’ll negotiate direct access to users’ data lockers only as needed. Then, by sharing data back to the customer — for example, sending a receipt to an “expenses” folder and an itinerary to a “calendar” folder — organizations will keep improving the value proposition.

- **Opt-in audience targeting platforms.** Marketers use a variety of audience targeting tools to identify and target their best prospects and customers. But these platforms have flaws: They aren't permission based; their data is often full of errors; and, at best, they’re only able to infer customer needs. A new breed of audience targeting startups takes a different approach: They let consumers choose to share their data and intentions in exchange for tangible benefits. Personal, a data storage and sharing provider, and Placecast, a location-based marketing platform, are two such vendors.
IN THE FUTURE, CONTEXTUAL PRIVACY EQUALS TRUST AND SUCCESS

How will these tools work in practice? Here’s how the chief marketing officer (CMO) of a pet products company — let’s call it Sensapets — might see things a few years from now. Like most companies, Sensapets leverages a wide variety of information about its customers, from what they buy to who’s in their social graph and how they interact with the brand. But there’s a twist: Like an increasing number of products, from running shoes to medical devices, Sensapets’ products include sensors that generate information about the people and pets that use them, plus apps that provide access to that information. So how should a brand like Sensapets practice contextual privacy?

- **Let customers use its website with SSO.** Single sign-on makes the registration process nearly friction-free, and it gives customers a real choice about which *identity* they want to use with Sensapets. Meanwhile, SSO also lets the company avoid storing passwords, thereby reducing the risk that hackers will gain access to sensitive customer data.
■ Give customers choices for how much data they share. Sensapets should let customers opt in to data collection, and it should provide preference centers that let them choose the products they care about, how frequently they want to receive communications, and what content they’re most interested in. This way, its customized advertising, emails, and landing pages won’t come as a surprise for its customers.

■ Buck the trend of “data hoarding.” By limiting its data collection and retention practices, Sensapets can mitigate risks like being forced to share customer data with a government agency, such as for a potential public safety inquiry about large dog breeds. Ultimately, the less data the company stores, the lower its liability will be in case of a data breach.

■ Partner with opt-in audience targeting platforms. By working with an opt-in, cross-channel data platform like Datacoup, Sensapets can better recognize customers both in-store and online and tailor offers specifically to them. It will be better off than competitors that are building propensity models based on browser and demographic data of questionable quality. And if regulators end up requiring it to purge tracking data that’s not opt-in, the company would be way ahead.

WHAT IT MEANS

THE PRIVACY WARS HAVE BROAD IMPLICATIONS

Think privacy is a nuisance you can ignore until the market forces you to pay attention? In fact, the “privacy wars” between consumers, companies, and governments affect more than just your brand’s trustworthiness, the risk for data breaches, and public relations headaches. They’ve got widespread macroeconomic consequences, too. Over the next five years, we believe that:

■ Even companies that improve privacy practices will see more scrutiny. No good deed goes unpunished, and firms should know that talking about privacy as a differentiator is likely to attract attention. As privacy vendor Evidon told us, “We have over 200 clients . . . who will talk [about our privacy solutions] glowingly off the record, but as public companies, it's much harder for them to talk publicly about how working with us brought them into compliance.” Google experienced this firsthand when it unified most of its services under a single privacy policy in 2012. The new policy is better, more simplified, and provides more choices, but the media didn’t report it that way.

■ Privacy and data practices will effectively become a nonfiscal trade tariff. If the US government’s NSA keeps amassing personal data and US-based corporations fail to get their privacy and security houses in order, American corporations will suffer in doing business globally. Already, some European vendors have been successfully winning enterprise customers because they host data in the EU rather than the US. Forrester estimates that the total cost of revelations about the Prism project to the US cloud computing industry alone could reach $180 million.
The battle for digital identity will bring privacy to the headlines again. Savvy marketers know that cookies are a poor way of identifying online users. Now, with a massive volume of Internet activity moving to mobile devices — and the recent discovery that the NSA was using a particular tracking cookie in its surveillance practices — the death of the cookie is imminent. Microsoft, Apple, Google, and others have signaled their intention to create persistent user IDs to solve the cross-platform user recognition problem. Companies will find that these providers are a new set of intermediaries they must count on for help identifying users. They’ll compete not just on the data they have, but on how well they address contextual privacy concerns. If you partner with the wrong one, you’ll be blamed for its transgressions.

Icon-based privacy tools will become popular. The work of firms like Disconnect is just the beginning. Mozilla (Firefox’s maker) is actively supporting that project; Google, Safari, and Internet Explorer will all support browser plug-ins that make privacy policies easier to read. These tools will show individuals, each time they visit a new site, what the company’s online privacy statement says, and whether it’s ever been reported for breach of privacy or misuse of data. In fact, we envision a “privacy markup language” that will make privacy policies more machine readable and will even trigger customer notifications when a firm’s privacy policy changes.

PIDM and privacy vendors will merge and create trust blacklists. It won’t take long for the emerging consumer PIDM services — data lockers and authorization managers — to identify new revenue streams by partnering with, acquiring, or merging with privacy technology firms to help consumers control where their data goes. These services will let users create “fake profiles” and use email aliases, obfuscating their real identities and interfering with customer and marketing analytics. (One solution, Abine, has already taken this a step further with credit card masking: The retailer never sees the customer’s real data, because Abine acts as a payment intermediary.) As adoption of these services increases, the services will begin to create privacy-offender blacklists to help users more efficiently utilize their tools.

As de-anonymization tools improve, more data will be regulated as PII. Everyone knows that fingerprints and retinal scans can identify an individual with near 100% accuracy. But did you know that your heartbeat, your gait, and even your writing style (and no, that doesn’t mean penmanship), are already considered “personally identifiable”? That may not seem like a big deal today, but soon security cameras will be able to identify you as a repeat store visitor simply by tracking how you walk. And the giant network of connected treadmills will have an accurate record of every time you’ve visited a gym with that equipment. As these tools and devices become smarter, governments will begin aggressively regulating what data can be collected, and for what purposes.
As the mobile mind shift grows, the desire to protect our devices will increase. Our research shows that 79% of US online consumers with smartphones are connecting to the Internet at least daily. As Marc Davis, founding director of Yahoo Research Berkeley and a founding member of the World Economic Forum’s Rethinking Personal Data project, has said, “[Our smartphones] are a social and cognitive prosthetic,” so the idea that they could be used against us causes friction between consumers and businesses. Already, consumers leave scathing reviews for apps that require access to too much data, or too many permissions. Companies that don’t build their mobile apps with contextual privacy in mind will lose customer confidence and — because they don’t have a place on the user’s device — will lose market share to competitors who do.

SUPPLEMENTAL MATERIAL

METHODOLOGY

We conducted a series of interviews with marketers, agencies, technologists, start-ups, product designers, and data services firms. We also spoke to academics and policy leaders in the field of privacy — from consumer advocacy to legal processes — relating to the collection and use of personal data. Special thanks to several Forrester Research colleagues who provided valuable insight and guidance on this report and the concept of contextual privacy: Carlton A. Doty, Nate Elliott, Anthony Mullen, Nicole Reitz, Heidi Shey, and Shar VanBoskirk.

For its North American Technographics® Media And Advertising Online Benchmark Recontact Survey, 2013, Forrester conducted an online survey fielded in June 2013 of 5,028 US individuals ages 18 to 88. For results based on a randomly chosen sample of this size, there is 95% confidence that the results have a statistical precision of plus or minus 1.4% of what they would be if the entire population of US online adults (defined as those online weekly or more often) had been surveyed. Forrester weighted the data by age, gender, income, broadband adoption, and region to demographically represent the adult US online population. The survey sample size, when weighted, was 5,012. (Note: Weighted sample sizes can be different from the actual number of respondents to account for individuals generally underrepresented in online panels.) Please note that respondents who participate in online surveys generally have more experience with the Internet and feel more comfortable transacting online.

This survey is part of our North American Online Benchmark Recontact System. Respondents who participated in both of our online benchmark surveys (part 1 and part 2) are invited to also participate in a series of follow-up recontact surveys that cover topics in greater depth and detail. The data from both online benchmark surveys (part 1 and part 2) is appended to each recontact survey’s data set so that data cuts can be performed across benchmarks and the recontact itself. Ultimately, this recontact system provides a more holistic view of consumer behavior and allows for more data-cutting opportunities than a standalone survey provides.
Companies Interviewed For This Report

<table>
<thead>
<tr>
<th>Abine</th>
<th>Experian</th>
</tr>
</thead>
<tbody>
<tr>
<td>Axiom</td>
<td>Federal Trade Commission</td>
</tr>
<tr>
<td>Agingo</td>
<td>Lively</td>
</tr>
<tr>
<td>Apthority</td>
<td>MapMyFitness</td>
</tr>
<tr>
<td>Automatic Labs</td>
<td>Mozilla</td>
</tr>
<tr>
<td>AVG Technologies</td>
<td>Neustar</td>
</tr>
<tr>
<td>Co3 Systems</td>
<td>OgilvyOne</td>
</tr>
<tr>
<td>Datacoup</td>
<td>Placecast</td>
</tr>
<tr>
<td>Disconnect</td>
<td>Privowny</td>
</tr>
<tr>
<td>DuckDuckGo</td>
<td>Progressive Casualty Insurance</td>
</tr>
<tr>
<td>Edelman</td>
<td>StartApp</td>
</tr>
<tr>
<td>enliken</td>
<td>TomTom</td>
</tr>
<tr>
<td>Euclid</td>
<td>TRUSTe</td>
</tr>
<tr>
<td>Evidon</td>
<td>UnboundID</td>
</tr>
</tbody>
</table>

ENDNOTES


4 Google has been found guilty of privacy law violations in at least nine countries. While the fines against it have been relatively minor, the company is now held to increasingly rigorous requirements with regard to training, privacy audits, consumer communications, and more.

5 Mondelez, the global snack foods maker, plans to launch its “smart shelf” by 2015. The shelves would contain sensors to determine the age and gender of shoppers, as well as whether they’ve picked up a product from the shelf, in order to show the shopper a customized ad on the display. Source: Clint Boulton, “Snackmaker Modernizes the Impulse Buy with Sensors, Analytics,” CIO Journal, October 11, 2013 (http://blogs.wsj.com/cio/2013/10/11/snackmaker-modernizes-the-impulse-buy-with-sensors-analytics/).
6 The FTC determined that Path collected the data without notice or consent, and it fined Path $800,000 because of illegal collection of personal data from minors. The settlement further requires Path to establish a rigorous privacy program and to undergo independent privacy audits every other year for 20 years. Source: “Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users’ Mobile Address Books,” FTC press release, February 1, 2013 (http://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived).

7 As we now know, things may be even worse: Some companies’ main network trunks have been deeply compromised by the government without their knowledge. Source: Susan Landau, “Making Sense from Snowden: What’s Significant in the NSA Surveillance Revelations,” IEEE, 2013 (http://www.computer.org/cms/ComputingNow/pdfs/MakingSenseFromSnowden-IEEESecurityAndPrivacy.pdf).

8 Open data is “a piece of data is open if anyone is free to use, reuse, and redistribute it — subject only, at most, to the requirement to attribute and/or share-alike.” Source: Open Definition (http://opendefinition.org/).

For additional information about open data for business, see the August 8, 2013, “Getting The Most Out Of Open Data” report.

9 Our research shows that consumers are talking with their wallets — 59% of US online adults take the time to read privacy policies at least sometimes, and a full third of US online adults who read privacy policies say that they’ve walked away from a transaction with a company because of trust issues. Source: North American Technographics® Media And Advertising Online Benchmark Recontact Survey, 2013.

Forrester’s data security and privacy playbook provides a framework for protecting data from a technical and governance perspective. Business leaders can point their privacy and security counterparts to one of the reports in our playbook for details. See the January 10, 2013, “Measure The Effectiveness Of Your Data Privacy Program” report.

10 For example, Forrester has identified that the 51% of US online adults that represent "green" and "super green" consumers are an extremely valuable segment of the population. For a detailed analysis of these green consumers, and how they are driving market dynamics, see the December 3, 2013, “Why Every Online Retailer Needs To Think Green” report.


12 In 2006, The Body Shop came under fire for “greenwashing,” after agreeing to be acquired by L’Oreal. By that time, however, the company had already created significant market traction for the sustainable personal health market, which the organization Lifestyles of Health and Sustainability (LOHAS) estimates is a $117 billion market. Source: Debapratim Purkayastha, “The Body Shop: Social Responsibility or Sustained Greenwashing?” ICFAI Center for Management Research, 2007 (http://backup.oikos-international.org/fileadmin/oikos-international/international/Case_competition/Inspection_copy_ICFAI2007.pdf); Lohas (http://www.lohas.com/about).
Most instances of multiple ratings refer to an R-rating at the box office with an NC-17 version released to home video. Recently, though, the producer of the film “Fifty Shades of Grey” has suggested simultaneous NC-17 and R versions of the move will be released to theatres.


The Physicians for Social Responsibility (PSR) has published a list of the top 100 dairies in the US and the status of their use of rBGH. Source: “BGH- (rBST-) Free Dairy Processors Top 100 List (as of 9/15/10),” Physicians for Social Responsibility, September 15, 2010 (http://www.psr.org/chapters/oregon/assets/pdfs/top-100-rbgh-free-dairies.pdf).

There is a business model issue at play in the privacy equation. Companies like Facebook, Google, and many publishers give away the “product” (i.e., services and content for consumers) so that they can sell data and advertising space to their real “customers” — advertisers. But most companies — retailers, insurance and financial services firms, and travel companies included — actually sell their goods and services to consumers, who are their actual customers. The companies in the former category will have a significantly harder time changing their privacy paradigm because their users’ data and eyeballs are effectively the product they are selling.

AB 370 requires companies to disclose whether they collect and/or share customers’ online activities “over time and across different websites”; they must also indicate how they will respond to “do not track” signals. Finally, companies must disclose information about both first- and third-party cookie practices on their sites and apps. SB 46 increases existing data breach reporting and notification requirements, and it extends the definition/types of personal information that are included in the requirements. Finally, SB 568 significantly extends privacy rights and protection for minors. The new law prohibits certain types of online advertising to minors, and it requires website operators to provide a mechanism for minors to access and delete information they have previously posted. Source: California Legislative Information (http://leginfo.legislature.ca.gov).

The portal (AboutTheData.com) is an initiative to show consumers some of the data that Acxiom has compiled about them, to provide education around how certain types of data are sourced and used, and to let users correct and/or suppress the use of these data points for marketing purposes. Forrester wrote about the portal in a blog post. Source: Fatemeh Khatibloo, “Acxiom’s Untied Kimono,” Forrester Blogs, September 6, 2013 (http://blogs.forrester.com/fatemeh_khatibloo/13-09-06-acxioms_untied_kimono#node-9717).

Limited retention does have some legal boundaries. Some types of data must be kept for extended periods, beyond their practical business or marketing use, for audit purposes. And in some cases, national and/or regional laws may require that certain data be retained in perpetuity.

Privacy by Design (PbD) is a framework that ensures that privacy and data protection are embedded through the entire product development process, from design to use and disposal of the product. More information about PbD can be found at Privacy by Design’s website (http://www.privacybydesign.ca/). The entirety of Mr. Iger’s letter can be found on Politico’s website (http://images.politico.com/global/2013/01/30/130130_disney_markey.html).

MIT and the Université catholique de Louvain, in Belgium, analyzed data on 1.5 million cell phone users in a small European country over a span of 15 months and found that 95% of users could be uniquely identified from just four location reference points (like a tweet or Foursquare check-in). Source: Larry Hardesty, “How hard is it to ‘de-anonymize’ cellphone data?” MIT News, March 26, 2013 (http://web.mit.edu/newsoffice/2013/de-anonymize-cellphone-data-0327.html).


According to the 2013 NAI Mobile Application Code, PII is defined as “any information used or intended to be used to identify a particular individual, including name, address, telephone number, email address, financial account number, and government-issued identifier.” Source: “2013 NAI Mobile Application Code,” Network Advertising Initiative, 2013 (http://www.networkadvertising.org/mobile/NAI_Mobile_Application_Code.pdf).

However, the National Institute of Standards and Technology defines PII more broadly, saying it includes "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.” Source: Erika McCallister, Tim Grance, and Karen Scarfone, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),” National Institute of Standards and Technology, April 2010 (http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf).

Forrester lays out responsibility assignments across marketing, business technology, and operations for developing such a task force. See the February 22, 2013, “Building Data Stewardship Is A New Customer Intelligence Imperative” report.
The data privacy standard shouldn’t be construed as the sole asset in a strong data governance practice. Instead, it should relate to and plug into the broader strategy for master data management and governance. A data privacy standard fits squarely into the Dissect phase of the framework outlined in the following report. See the January 15, 2013, “Know Your Data To Create Actionable Policy” report.

Forrester’s data management playbook can help organizations get started. See the July 2, 2013, “Transform Your Organization With Strong Data Management” report.


Consumers are leaving an exponentially growing digital footprint across channels and media, and they are awakening to the fact that marketers use this data for financial gain and this will only grow with the digital self. So individuals will increasingly want to know when data about them is being collected, what is being stored and by whom, and how that data is being used. As a result, a nascent industry is forming, with the promise of giving consumers control over their own data. See the September 30, 2011, “Personal Identity Management” report.

Forrester wrote about preference management in 2009. It has taken nearly half a decade, but firms are finally beginning to invest in preference as a key part of their customer engagement strategies. See the July 22, 2009, “Marketers: Stop The Abuse! Adopt Preference Management” report.


On December 10, 2013, The Washington Post reported that the NSA had gained access to at least one particular Google tracking mechanism, called the PREF cookie, which enables websites to uniquely identify a person’s browser. Source: Ashkan Soltani, Andrea Peterson, and Barton Gellman, “NSA uses Google cookies to pinpoint targets for hacking,” The Washington Post, December 10, 2013 (http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/).
People must manage an exploding array of digital content that they create or are responsible for, both at work and at home. Forrester calls this collection the digital self, and we believe that the tools — like services for file sync or notes — are evolving into a full ecosystem of services for individuals. See the September 3, 2013, "Services For The Digital Self" report.

Abine's MaskMe service masks email and phone numbers in online fields at no cost. Users can upgrade to a paid version for $45 a year, which enables disposable "masked" credit card numbers. The merchant never gains access to the individual's credit card or, in some cases, billing address. Masked card purchases appear on the consumer's regular credit card statement as charges from Abine.


For more information about when and how consumers interact via mobile, see the April 19, 2013, "The Mobile Mind Shift Index" report.

About Forrester

Global marketing and strategy leaders turn to Forrester to help them make the tough decisions necessary to capitalize on shifts in marketing, technology, and consumer behavior. We ensure your success by providing:

- Data-driven insight to understand the impact of changing consumer behavior.
- Forward-looking research and analysis to guide your decisions.
- Objective advice on tools and technologies to connect you with customers.
- Best practices for marketing and cross-channel strategy.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Customer Insights Professionals

As a data-driven marketer, you’re responsible for capturing, managing, analyzing, and applying customer knowledge and insight. You draw from all sources of customer data, marketing automation technology, and customer analytics to improve marketing and business performance.

« CHARLES IBRAHIM, client persona representing Customer Insights Professionals