Chapter 12

Trust: The New Currency

You have zero privacy anyway. Get over it.

Scott McNealy, CEO, Sun Microsystems

Up to this point, we have extolled the virtues of new technology that can improve our homes, health, transportation, communication, work, lives and the planet we live on. Contextual technology is helping us explore outer space and the inner body. We have spoken to hundreds of people and looked at hundreds of technologies, and we firmly believe that adding context will make the world an easier, more efficient, cleaner and more productive place.

However, we’d be negligent if we didn’t point out that the price we pay for many of these benefits is our personal privacy. Every new piece of technology we adopt requires us to consider that price and how it is exacted. Some companies are not as transparent about how they take and use our private information as we believe they should be. We think it is imperative to know what the companies we deal with do with the data we are required to give them.
Loss of personal privacy had been going on for a long time before Scott McNealy made his observation. In the early days of the home telephone, “party lines” enabled your neighbors to listen in to your conversations without your knowledge. Your social security number used to be a secret between you, your employer and the federal government. Now you need to share it to get a Comcast account. Your credit card numbers are stored online where they are often shared between vendors, without your knowledge. When you clicked that button to consent to a Terms of Use Agreement, you probably did not quite understand the implications hidden in the legalese.

This chipping away of personal information accelerated when we moved online, where our Facebook posts about a vacation can alert a burglar to an opportunity, and photos of a loved one may attract a stalker. In the Age of Context, mobile and wearable devices keep track of our every motion, even as we sleep, and the rate at which our privacy is eroding grows exponentially.

We did not fully understand the scope of the privacy issues people face when we started work on this book. Our goal was to tell you about incredible new technologies that can understand you well enough to predict what you will need next and to automate many mundane tasks. But with each chapter we found new privacy issues, and some are too serious to brush aside.
While we were busy searching the world for mobile, social media, sensor, data and location technologies, the issues of government surveillance became a prominent national issue in the United States. As the names Bradley Manning, Dzhokhar and Tamerlan Tsarnaev, and Edward Snowden emerged from the headlines into the national consciousness, public attention came to focus on the role of the secret Foreign Intelligence Surveillance Act’s (FISA) court, the electronic surveillance of millions of Americans under a National Security Agency (NSA) data-mining operation called PRISM and so much more.

We are just a couple of tech enthusiasts, and some of these national issues would normally go well beyond our purview, were it not for the fact that the same technologies we are extolling are being used secretly to watch people. Data about our searches, social media interactions and even our cell phone conversations is being collected for purposes far different than we had imagined.

Most people we talked with have strong feelings about this, as we do. But we are conflicted about a solution. We want a safer country. We want to be comfortable attending large gatherings such as the Boston Marathon. We want small cells of conspirators to be detected and deterred before they can take diabolical actions.

How much citizen privacy should be sacrificed in the name of national security? We really do not know the answer. What we have come to realize is that the conflict between security and privacy will not be easily or quickly resolved.
We do believe, however, that people would be far more comfortable if government were more transparent with the people they are supposed to serve. For example, Google wrote an open letter to Attorney General Eric Holder in late July 2013, asking for permission to reveal how many of its user files had been subpoenaed under authority of the FISA court. No answer was forthcoming as of this writing. Daily revelations make us aware of more and more surveillance, resulting in less and less trust.

It leaves people wondering: Is Big Data watching us? The answer is a resounding “Yes.”

We think the benefits we gain from contextual technology are worth the cost of the loss of some of our personal information.

Not everyone will agree with us. Where there is common ground is that the public needs to be more aware of what information is being collected, and we deserve to know what will be done with that information.

Even more important, people should be allowed to opt out whenever they find that the privacy costs are just too high for their personal tastes. And it should be easy to do.

We believe that greater transparency by businesses and government will lead to higher rates of customer and citizen participation.

What bothers us is the sneaky stuff.
The Right to Go Silent

Always-on technology brings clear advantages. It is convenient to have your personal contextual assistant (PCA) see that it snowed while you slept and wake you up early so you’ll make it to work on time. But shouldn’t there be an easy way to take a break from the relentless eyes, ears and data collectors that are part of life in the Age of Context?

Many contextual products already provide features that enable you to selectively keep some activities private. For example, NextGuide, the contextual TV program location service, lets you share what you watch and like with Facebook friends—or go private so that your co-workers don’t know that you have a secret penchant for kickboxing.

We have mentioned many products that offer such controls, but some of the most advanced products do not yet provide such options. We believe that both Google Glass and the Moto X phone will be flagship products in the new Age of Context, but both have features that concern us.

Glass watches what you watch. It has a sensor that records data on what you look at, how often and for how long. Moto X has a microphone that never turns off, even when the phone’s power is turned off. That arrangement allows you to conveniently issue voice searches through Google Now, but it also means that the phone never stops listening. Providing the ability to selectively opt out, or go silent, is essential to earning and keeping our trust.
Plain Speaking

Millions of people use Fitbit, Nike Fuelband and other devices to monitor every aspect of their bodily functions in an effort to become healthier.

The unanswered question becomes, who owns such potentially sensitive data? Who gets to share it? Some users, we are told, are so obsessed with counting every expended calorie, that they even wear the device while making love. Seems mildly amusing, until we started wondering who owns that data and who has the right to share it. Could it be used as evidence in a divorce case?

Sensors meshed together in dissolvable tattoos are used on paralyzed patients today. In the near future, those sensors are likely to monitor all sorts of bodily functions. Researchers are examining them as early detectors of cancers. Sending such data directly to our doctors makes sense. But do our insurance companies get to see it before we do? How about our employers, who often pay for most of the insurance? Who gets to decide?

From our investigation it seems the issue of personal data ownership is murky and getting murkier. Shel Israel has been a diabetic for many years, jabbing his finger a few times every day to measure his blood sugar. Every six months he brings his glucose meter to his endocrinologist, who extracts and analyzes the data.
His pharmacist recently informed him that a new California law requires him to share his data with them as well or his insurance coverage will be dropped, raising the monthly cost from about $8.25 to about $165. Who is behind this law? What is being done with medical data that is gathered at a local pharmacy and reviewed by state auditors? Israel is reasonably sure that the state’s 3.5 million diabetics were not asked what they thought.

It seems self-evident that we should own our own data and that any third-party should need our permission to use it, and our refusal should not trigger financially punitive measures.

The definition of privacy as the right to be left alone should apply to more than medical records. It should apply to all data, including our photos, conversations and credit card balances. But, when we agree to those boring terms-of-use agreements, we—often unwittingly—yield to vendors the right to do with our private information whatever they wish. When you post that photo of you celebrating a bit too much on Instagram, opting to share it only with your friends, Instagram claims it has the right to reuse it—and it apparently does—but in a democracy, shouldn’t users be asked?

We also believe in the user’s right to plain language.

If we are going to voluntarily yield personal data, then plain, straightforward language should be used in the required opt-in agreements. The repercussions should be spelled out and explained in great depth.
The loss of much of our privacy may be inevitable, but the lack of transparency is something for which we can and should hold companies accountable.

Pushing back on this point may get results faster and more easily than some people might think. But over time, we will remain the most loyal to the companies that earn our trust and do not betray it.

**Human Override**

EasilyDo, one of the PCAs we like, uses a “Do-It” button that gives you an opportunity to override your software assistant before it performs tasks on your behalf. Google Now, the most popular PCA, does not have the equivalent of a Do-It button. We think Google Now needs one before we can trust it with our personal information.

We told you two of the most disturbing user privacy stories we found in Chapter 9 on PCAs. First, Dave Winer talked about picking up a female friend at the airport when Google Now warned him about her delayed flight, connecting him to her flight information without any input on his part.

Then Steve Brady related a similar story where Google Now presumed he was in a more advanced stage of a relationship with a woman he knew than was actually the case and the mobile app started sharing her private data as if they were committed partners.
For users to trust Google Now in the long run, the danger of personal contextual assistants giving out privileged information must be far less than the threat of a human assistant doing so.

All personal contextual assistants should be designed to ask for permission and not make assumptions, until a user pattern is well established and the owner specifically grants certain permissions that would remain in effect until cancelled.

No one wants a PCA that rats you out. You cannot fire them the way you would an indiscreet employee, but you can stop using them and stop trusting their manufacturer.

**Privacy Is Subjective**

Privacy is complex, fluid and granular. How much of it we want depends on many variables. Facebook used to let people respond to their relationship status as “It’s complicated.” We think the same option can be used for privacy.

As parents, we would be willing to yield a lot of our children’s location and personal data if it would ease their suffering from diabetes or asthma as we talked about in our chapter on Contextual Health.

However, we may not want a security sensor that can record data or movement in our bedrooms. We may not mind Facebook electing to share a cute picture of our kid at a school concert, but most people would not want photos of their children in front of their houses where addresses are visible posted in public spaces.
Such user-empowering controls are not technically hard to accomplish. As contextual technology pushes forward with relentless speed of development, certain safeguards seem to be getting overlooked or bypassed.

For example, if a college student posts a photo showing how he over-celebrated at a graduation party, technology exists for an online service to display a pop-up dialogue box to ask: “Are you sure you want to post this? This photo may be harmful to you in a job interview, or when you ask your parents to subsidize your summer vacation...”

Warnings about risks seem to have been brushed aside in recent times, even though we are entering increasingly risky times. In the Age of Context we seem to be unnecessarily performing risky tasks without a safety net.

**Trust Is the New Currency**

We believe the most trustworthy companies will thrive in the Age of Context, and those found to be short on candor will end up short on customers. Transparency and trustworthiness will be the differentiating factors by which customers will make an increasing number of choices.

Most of the products we have examined in this book have one or more competitors already; the remainder soon will. Competitors will leapfrog each other’s capabilities—whenever one product offers a desirable new feature, the others will soon offer a similar or slightly better one.
In mobile phones, iPhone had a clear functionality edge for a long time, but as we write this, Android has equaled or surpassed iPhone’s features in many ways. Now the Moto X has come along, which may set a whole new standard because it has incorporated contextual functionality into its operating system.

The key point is that despite the volatile nature of the market, many products will become commodities earlier in their development cycles than was the case with previous technologies. For example, we looked at about ten PCAs. Each of those we highlighted had at least one unique feature, but it seemed likely that competitors would be able to match them pretty easily. People will probably choose just one PCA and stick with it, even if one feature lags for a few months. The same tendency for people to commit to one product and stick with it affects wearable devices and home management systems.

If features aren’t the deciding factor, how will we choose? We think that most people will select the products made by the companies they trust the most. The most transparent companies—the ones that give the user privacy options they can understand and the option to turn apps and devices off and on as they see fit—will be deemed the most trustworthy. Similarly, companies whose products warn users before they do something that may embarrass them will be valued and trusted, gaining their loyalty along the way.
Today, Google seems to have taken a leadership position in this area. They have posted a single page where you can see the company’s privacy policy as well as all the types of data it collects on users. If you visit that page, you may be surprised at how much Google knows about you.

Although Google may lead in this area today, the previously mentioned serious and unresolved Glass and Moto X privacy issues are evidence that every company has at least one Achilles’ heel in the area of privacy.

If we were developing a long-term company strategy for the Contextual Age, we would start by matching everything Google has done in transparency, and then try to surpass it. Users would certainly embrace such a competition.

We think business leadership, in the short term, will require understanding that more is gained than lost by shining some sunlight on a few shady areas. Some organizational decision makers have grown comfortable and have prospered in the shadows. Some may opt to lurk there. But that’s not where their customers are comfortable. And ultimately, profitability lies in the customers’ comfort zone.

In our view, the shadow-lurkers may grab some sweet, low-hanging fruit, but in the long run they will lose to companies like Google and other like-minded businesses. Openness and transparency create a significant opportunity for every startup that has giant-killing already etched into its organizational DNA. If we are right, then the Age of Context will give us an open new world.