CHAPTER 14

A Vision of the Future: The Privacy Engineer's Manifesto

There is one thing stronger than all the armies in the world, and that is an idea whose time has come.

—Victor Hugo

In this final chapter, we propose that this beginning framework for privacy engineering should become amplified like the open mouth of a megaphone (to invoke an oldie-but-goody technology) to enlighten and guide future data privacy and security professionals in a world of increasing pervasive computing. Taken together, the known standards and lessons from past waves of innovation can lead to an explosive and productive information society; but we need to acknowledge the historical certainty that individuals do, in fact, desire a certain degree of freedom to live a life of their own determination without excessive government or corporate interference. These same individuals may wish to communicate, socialize, and receive personalized services. At the same time, individuals should be free from "services that penalize" their users (i.e., those that are encumbered by excessive peeping, overenthusiastic assumptions about preferences, a false sense of safety, undue influence, a filter that causes an information bubble, or other dystopia-like scenarios).

We are creatures of ever-changing context. To meet requirements based on values of ethics, safety, morality, and even fun and laden with every imaginable deconstuctable, predictive, or analytical dataset, we must design forward and fearlessly, with a solid foundation grounded in the experiences of the past. Passive drifting into ever fewer controls and greater obscurity of purpose is not a viable option.

So, this chapter considers two visions of the future: one, where we continue our present technology-centric ways, drifting relentlessly toward chaotic mismanagement of data, or two, where we learn how to thrive in a world with unfettered volumes of data. In this privacy-engineered world, metrics are available to create, manage, and extend information markets that are available to enterprises and individuals alike.

Finally, we propose a privacy engineer's manifesto. A good revolution requires a manifesto, and what we've described in this book documents nothing short of a revolution in how humans look at themselves and think about their world. Innovation in data governance over intellectual property and personally identifiable data (and the gray

overlapping spectrum including machine data between), technology enhancements, and societal pressures affects the way we look at privacy. The question remains: Will our views on data privacy drive us forward into greater innovation and markets or shall we, as a global community with differing views on data, retreat into informational and legal stasis, with little or no pragmatic protections for data assets?

Privacy can become a strong platform for relating to customers and users upon which individuals can stand to communicate with governments and commercial enterprises—if we make the conscious decision to create that reality.

Where the Future Doesn't Need Us

In 1999, Scott McNealy, cofounder and CEO of Sun Microsystems, Inc., infamously harumphed "You have zero privacy anyway. Get over it!" in response to questions about technologies designed to help devices and users communicate to do things like printing documents remotely.[1] Although that technology may seem benign compared with wide-scale open datasets, government intelligence gathering, and wearable computing, the dialogue remains an open one today. Is there an either/or choice to be made between new features, old-time spying, and personal respect and privacy? Has an information-hungry world simply vetoed data protection?

Perhaps data privacy—or any sort of privacy—is simply too hard to protect; perhaps we should accept living in a surveillance state and submit any rights to self-determinism to some higher power that will keep us safe. Perhaps the root of substantive privacy belongs to some Orwellian, Big Brother entity, and our technology, legal, and procedural models should reflect our placid acceptance of an omniscient, "public," and centrally organized and governed IT infrastructure.

It certainly can *appear* that technophilliacs and young people have decided that the future is one where all information is "free" (i.e., neither owned nor managed by them) and that no one should have anything to hide. The truth, however, is likely far different from the myth. The real answer is more complex and a lot more exciting where young people routinely present themselves how and to whom they see fit. Technophiles reject and actively protest overreaching interference and peeping by governments and technology features and settings.

CALCULATING THE COST OF PRIVACY

By Raj Samani, Vice President, Chief Technical Officer, EMEA, McAfee

Society demands privacy, yet ironically many seem happy to share their deepest secrets to the world for nothing more than a handful of magic beans and the promise of a new feature. It must seem incredibly frustrating for professionals who dedicate their working lives to preserve privacy, when again and again consumers hand over their data like it is absolutely worthless.

[1] www.wired.com/politics/law/news/1999/01/17538

I experienced this frustration many times, but none more so than in 2012. A plucky confectioner decided to run a promotion giving away "free" chocolate. The "cost"? Their personal data of course! Perhaps more remarkable were the long lines of willing participants, and in the 10 minutes I stood there, incredulously not one single person read the privacy statement collecting cobwebs just beside the chocolate station.

This experience compelled me to write an article titled "How Much Do You Value Your Personal Data?"[2] in which I made the bold claim that the disparity between the perceived value of personal data and its actual value was at its widest.

How wrong I was! At the time it did not cross my mind that things could be worse than consumers perceiving their privacy as being worth less than a bar of chocolate, but sadly in the past 12 months the perceived value has dropped to zero. Recent retail experiences would suggest that not only is the value at its lowest, but there is no shortage of consumers willing to check out of the personal data economy just before it really takes off.

Most people use corporate loyalty cards, justifying the value they provide in discounts as a fair exchange for their personal and transactional data. Equally, many use social networks with the value they provide seen as a fair exchange. Others may argue, at the very least, there is a value associated with their personal data, be that discounts, or belonging to a social network, amongst others. However, recent experiences would suggest that some organisations are now charging for their loyalty cards, sorry I meant double charging. Not only are consumers expected to pay with their data, but they are also being asked to pay via monetary means. Furthermore, it would appear that 200,000 consumers were already members of one particular scheme!

This is not an isolated example, with more than one retailer actively double charging consumers who seem more than willing to pay twice. What is clearly evident is that while large corporations and privacy professionals clearly understand the value of personal data, the consumer is facing personal data bankruptcy. Sadly, this decline will mean for many that they will fail to realise the financial benefits of this emerging economy.

Twitter @Raj_Samani

The collection of thoughts presented in the sidebar may seem better suited in the discussion in Chapter 13 regarding value models. Upon examination, the ideas and attitudes of today's consumers are instructive for the privacy engineer. In the store loyalty example, the consumer pays twice. First, the customer gives away his shopping data to the retailer. Second, he pays to have the card at all. Because the system is neither

[2] www.telegraph.co.uk/technology/internet-security/9605078/How-much-do-you-value-your-personal-data.html

customer centric nor does it clearly disclose the ultimate purpose for processing of the customer data, it seems likely that the current system has deployed few, if any, privacy engineering techniques. In this environment, the enterprise risks customer loyalty and trust by continuing to take advantage of its customers rather than providing real and transparent value.

It may be possible for retail brands to be strong enough to withstand charging its customers for giving away their own data. However, once these same consumers are faced with the slimmest margin of choice or price variance, the customer churn for those employing such tactics becomes intolerable. Alternatively, the enterprise may have to flatten its margins, pay a premium to maintain brand stickiness, or employ other costs to compensate.

Instead, a data scheme deploying fair information principles should be a better predictor of success and, thus, a better longer-term investment. The customer would be more engaged, the enterprise at less risk of disclosure of embarrassing practices, and the systems protecting data can be engineered accordingly.

Even Social Networks (and Their Leaders) Get Cranky When Their Privacy Is Compromised

To continue the interesting scenario of a future where each person is reduced to an object of data mapping and subject to the data observations of others, it is worth exploring how privacy can fit into current social networks.

The earliest days of the now infamous social networking site, Facebook, is a fascinating example of how data privacy can actually act as a business accelerator to start ups.

Facebook's current privacy profile is, perhaps, best known for its founder's rather glib statements about privacy's demise and the many governments worldwide that have investigated and attempted to regulate its privacy settings[3] and advertising models. But the history of Facebook and its implications for innovation is the more interesting story for the purposes of this chapter's discussion.

Social networking, blogging, and other online sharing began before Facebook became the dominant player in that market. In fact, MySpace, an early dominant force, was once the mainstream social sharing platform for music, gossip, meeting friends—and strangers. It has since become more of a music specialty boutique. In its heyday in 2006, the site was lambasted for failing to protect users from predators and peepers. Meanwhile, start up Facebook sold itself as the velvet-roped "in" place for "good" kids with .edu e-mail addresses. Only certain kinds of kids were allowed on the site, and users had to have specific school .edu domains to be allowed on the platform as a "Friend."

The ivy and elite schools that were acceptable circles for Facebook acted as their own type of authentication and limit to the platform—you may call a boy disgusting for gawking at girls in his college dorm, but he'sa well-heeled fancy school kid and, therefore, okay. Privacy of a sort was protected within these elite social and economic circles. Similarly, the ad business that would pay for the "free" use of the site was nowhere near

[3]See Canadian PIPEDA Case Summary 2009-008 at
www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.asp

the current sophisticated online behavioral models nor tracking capabilities of the same company, a mere decade later.

The controls for privacy grew more complex and nearly unfathomable to the average user. The social "circles" circumscribed by the social network became ever larger while the original controls and protections for information shared on the Facebook platform have eroded. Accordingly, users and regulators have increasingly grown weary of constant change and eroding policies regarding the monetization of the personal information of social users.

Irony still rules the day in the evolution of social and ad-based businesses. In a recent California conference, the CEOs for Facebook and Yahoo! were asked about revelations regarding US government activities. Facebook's Mark Zuckerberg's response should be very interesting to any privacy engineer. According to the press coverage, "Zuckerberg said the government had done a 'bad job' of balancing people's privacy and its duty to protect. 'Frankly I think the government blew it,' he said."[4]

Several of the CEOs who claim that privacy is an artifact of an earlier era or that it is no longer a necessary social norm have purchased extraordinarily expensive homes that surround their own suburban lodgings. It seems that their own behavior and desire for privacy remain of social and personal value. In these cases, architecture for privacy can indeed be inferred in the most literal sense. The extra homes and real estate are the ultimate in "hardware" protections for privacy.

This chapter concludes—as a capstone to the entire book—with a manifesto that summarizes how seemingly opposing motives of creating corporate profit, maintaining public safety, and respecting individual privacy can live in harmony. The manifesto provides some simple guiding principles and a vision for creating value in the complex world of product development where user needs and corporate motives must find a meeting grounds in mutual respect.

Let's Remember How We Got Here

Privacy is not a new concept. It has been around since before biblical times in some form or another. However, modern technologies such as databases and the Internet browser have changed some of our ideas about privacy in the sense that they have enabled a cyber world in which one's neighbors are faceless and powerful. Although the intent of an organization may be simply to extract value and intelligence from PI, sharing and using the data are much easier and more ubiquitous than before. It is the speed and reach of today's information age technologies that make the risk of misuse more noteworthy. There is no dispute that preservation and innovation around data protection or privacy are challenging and complex. Only the smart and courageous or, perhaps, adventurous and entrepreneurial, may wish to venture into this arena. No one ever said this was going to be easy.

In the opening chapter, we discussed how the boundaries surrounding an organization's information systems and data have become much more permeable in the past two decades. These advancements have opened up information systems so that people, devices, and systems are now nearly seamlessly connected. Today's users not

[4] www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance

only have access to a vast amount of information but also typically pay a price for it in terms of sharing their personal information with or without permission or contextual understanding.

The aftermath of this sea change is that vast troves of data are now collected by applications and web sites, creating an opportunity for organizations to mine that data and profit from it. Analysis of this data enables products and services to be tailored to each user's unique personal preferences, but more often, the "personal" preferences are actually an enterprise's guess at the type of product, service, or information that that enterprise wishes to push. Marketing promotions can also be carefully targeted to very fine-grained audiences or even individuals. Although this may have some limited benefits to users, it often creates a risk that personal information might be used inappropriately or neglected by an enterprise, resulting in the additional risk of loss or theft by malevolent third parties.

Privacy regulations have grown out of the need for consequences for organizations that may be tempted to misuse personal information. What we're striving for in today's information economy is to re-create a sense of mutual respect so users feel they can trust how their information will be used.

Privacy Is Not a One-Size-Fits-All Formula

There is a broad spectrum of acceptable privacy policies for complying with today's regulations, and many approaches to privacy can fall within the spectrum. The spectrum ranges from a scenario in which user choices about privacy are predominantly controlled by the organization vs. a scenario that represents almost complete freedom of choice for users. There are pros and cons for each approach, and an enterprise's approach will depend on many different factors. Each organization must decide which point on the spectrum best serves the needs of its community.

The organizational control scenario taken to the extreme can amount to a Big Brother approach: In this extreme side of the spectrum, users' decisions about privacy are turned over to the organization and thus users are basically submitting to a higher power that determines the best way to process personal information and ensure its safety. In this scenario, the IT infrastructure and applications are centrally governed and are designed to make "safe" choices for the user on his or her behalf. Users do not have to spend time thinking about privacy options or how much sharing to allow for their personal information. There will be options available to users, but most decisions will have preset defaults that the organization has determined are best for users. Where this scenario is deployed with a high degree of transparency, accountability to the user for error and a healthy respect for the ultimate uses of data, an organizational control method can work for the benefit of both users and the enterprise.[5]

An example of this scenario can be seen with medical records. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that health care providers follow strict procedures to protect patient information. Health care providers were collecting patient data long before HIPAA was enacted. Most were very careful about

[5]The new OECD privacy guidelines (2013) tend toward more enterprise data protection responsibility. If the enterprise fails in its responsibility, some legal liability would be expected. www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

protecting this data even though there was no law specifying how to do so. If health care patients want service, they have no choice about disclosing their personal information to the health care provider. They are thus submitting to a higher power to protect them and must essentially trust the health care provider to keep their data safe.

The biggest benefit to users in this scenario is that it requires very little effort on the part of the users. There is no need to study the privacy options and make choices. In theory, the health care providers can do a better job of understanding what's best for the users, but this requires that they have the users' best interests in mind. The enactment of HIPAA is an attempt to collectively govern the health care providers and make sure that providers do not misuse the information or fail to properly safeguard it. The US government is watching the watchers, so to speak. There are stiff penalties for noncompliance, so health care organizations pay close attention to HIPAA. The enactment of the law is an attempt to enforce proper ethics and moral standards.

At the other end of the spectrum is a scenario in which the user is given great freedom to share personal information and almost total discretion about what he or she would like to share. Social network sites can be an example of such a scenario. Many of the choices in social networks are set by default to enable broad sharing when the user does not specify a preference. The social network enterprise can argue that the entire intent and purpose of the site is to facilitate "open" sharing and, thus, may believe that the default to share settings are understood and even desired by users. For users who want to use greater discretion, such networks may offer options for limiting the sharing of information, but these choices require users to take action to learn how to implement the choice. Users must take the initiative if they want to manage their privacy settings.

The main benefit to users for the social sharing scenario is that users have greater freedom of choice. The massive potential downside to these social sites is that currently an information asymmetry exists where users do not have simple-to-use, clear, or transparent controls that result in reasonable protective outcomes. Additionally, many current social sites have buried analytics and algorithms used to process and make decisions on behalf of users and sell and resell personal information with no participation on behalf of the user in this economic boom. The users become, typically unwittingly, inventory rather than customers, and the actual economic drivers, those buying and selling advertisements, become the Customer who must be Obeyed.

For savvy users who can easily understand the impact of their choices, there are clear benefits to being given the freedom. Less savvy users tend to fail to research their options and typically go along with the default settings without really understanding the implications. Governance is essentially performed at the societal level in this situation. If enough users get upset about a change in privacy policy, they can take a stand together and rise up against the institution to ask for changes in how PI is managed or how privacy options are presented, or they can rely on regulators to step in on their behalf.

Does this situation create risk for the institution? One potential risk is that the early adopters of the technology will drive the future direction and enhancements. This might mean that the system will evolve to meet the needs of its early users but miss emerging market opportunities for users who might prefer a different approach to privacy. Another potential risk is that users could argue that they are governing the PI and thus the data should be considered a joint asset of all users rather than an asset of the institution. Would users then be eligible for a percentage of the profits from the organization's use of the data? And would the user community have rights to the data if the institution dissolved?

Most environments will be somewhere in between these two scenarios. You may decide that it's best to give significant freedom to your users or you may want to closely manage the usage and sharing of data. Perhaps your organization will want to set defaults that limit data sharing unless a user intentionally chooses something different. Woe betide the company that fails to contemplate or plan for the changing character of its users or business model.

As you choose your approach, be mindful of how your users will perceive your approach and how your approach will affect your organization's future vision for itself. Regardless of what your approach is, it will be important to be transparent to users and ensure that there is a fair exchange with users in terms of the value provided by your application or service.

Innovation and Privacy

The opportunities for innovation around privacy are almost endless and can span the entire product lifecycle from early product design through marketing, distribution, and support. Rather than try to summarize the different ways you could innovate around privacy, we'd like to think about where the future might be headed and what you can do to take action to move in that direction.

First, let's consider what makes a product innovative. Most of the great product and service innovations throughout history were not products that customers were already asking for. They were products—such as the Java programming language and the Apple iPhone—that made new markets, not because they were completely new inventions, but because they took a new approach to meeting a customer need.

The Java programming language, for instance, had many similarities to C and C++ languages. The uniqueness of Java was its ability to make code completely portable across operating systems and platforms. Thus it offered a new benefit while carrying forward the familiar syntax of existing and popular programming languages. Similarly, the iPhone was not the first cell phone, but it was the first one that was really integrated with Internet technologies in a way that made it easy for customers to understand and use these new technologies.

An earlier example of innovative or disruptive development is the combination of recordable media and entertainment. The VCR vs. Betamax war was the technology side of the revolution. The real innovation, however, that upended the entire entertainment industry and paved the way for new technologies like TiVo and other digital video recorders and business combinations like streaming video rentals, was the ability to use recordable media to easily "time shift" or play back entertainment when and where the user desired. All of these products and innovations have a common thread in that they met a need that had not yet been anticipated by the customers themselves. If you want to do more than just satisfy your customers, you have to anticipate their desires and deliver something that is different from that offered in the mainstream market.

So, what does this have to do with privacy? If you agree with the concept that we've reached a point where privacy requirements must be integrated into a product and cannot be just an afterthought, then you realize that how you address the privacy needs of your users must be part of your product development process.

True innovators around privacy will be those that build products that anticipate users' desires. For example, it's feasible to build a privacy tool that makes choices and suggestions for the user by making inferences from the user's past choices. In the field of online radio, Pandora has invested in such an approach and has designed a product that makes music selections for users based on an in-depth analysis of their past choices.

What's interesting about Pandora's approach, which they call the Music Genome Project, is that it has analyzed the musical attributes of hundreds of thousands of songs to create a database that can be used to match listener preferences against other songs the listener is likely to enjoy. Users are served up songs on their radio channel based on their individual tastes in music rather than based on simple categories such as music genre or artist name.[6] Like everything else, there are privacy risk/reward tradeoffs with a Pandora approach.

A similar approach could be taken with privacy. If a broad base of user preferences about privacy were captured, it could be possible to analyze these data and find common characteristics about privacy choices and thus predict a user's preference in a given scenario. This would allow an application to set privacy defaults based on a deep understanding of the user's privacy choices. Alternatively, the application could also present privacy options to users in ways that required only a minimal amount of clicks if the preference were accurately predicted. Each choice made by the user would add further accuracy to future predictions.

This is just one example of how a product might anticipate the privacy needs of its users. There are many other ways to innovate and open new market opportunities. It's nearly impossible to predict what the next big thing will be in the technology revolution, but we can be pretty certain that there *will* be a next big thing. It's our belief that privacy will be an integral part of the next wave in the technology revolution and that innovators who are emphasizing privacy as an integral part of the product lifecycle are on the right track. The sidebar delves into the idea of privacy needs.

PRIVACY NEEDS TO EVOLVE BETTER DECISION-MAKING MECHANISMS

By Dr. Eric Bonabeau, PhD, Chairman, Icosystem, Inc., and Dean of Computational Sciences, Minerva Schools at KGI

Privacy is that sense of control and safety you have when you know you can share information about yourself selectively and knowingly; when you know, often incorrectly, that your personal information will not fall into the wrong hands—scammers, spammers, nosy employers, overbearing parents, unforgiving peers. It is a fundamental human need, and yet it can be violated in an instant. Privacy has been a topic of social psychology for a long time, but there is an urgent need for a new cognitive framework in an age of permanent connectivity. If decisions affecting privacy were

[6]"How Pandora Radio Works," Julie Layton, May 23, 2006. http://computer.howstuffworks.com/internet/basics/pandora.htm.

complex 20 years ago, today the situation is beyond human comprehension because privacy is an emergent property resulting from myriad decisions, conscious or not, combining and interacting in ways that have become impossible to predict. Would E. M. Forster still urge us to "only connect"?

Today, more than ever, with powerful tools at our fingertips, there is a tension between our desire to connect and the fear of indelible digital trails we may one day regret leaving behind. But most often we push away the fear—it can't happen to me, or it won't, or I don't care. And we succumb to the temptation and give away information about ourselves. In fact, the most likely scenario is one where we are not even aware of our loss of privacy and its dangers, where the fear, if it exists at all, is diffuse and unattributable. Therein lies the privacy conundrum: privacy as we experience it today is misunderstood as a barrier between an individual and her desire to connect, or, also incorrectly, as an annoyance she will brush away in one instant, paving the way for a lifetime of unintended consequences. We need ways to make better decisions about privacy. To change this unfortunate state of affairs, there are a few things we can do that will yield a disproportionate return on investment:

The first is to recognize that privacy is, or should be, to a large extent, a topic of the behavioral sciences. Our sense of privacy is derived from being part of complex sociotechnical systems in which we have to resort to simple, probably inappropriate, heuristics to deal with all these little decisions that need to be made. They have been reduced to the deceivingly simple choices of opt-in and opt-out, install or cancel, a choice architecture that masks its deep and potentially dark consequences. The menus of privacy options available to you when you set up online accounts range from the binary ("our way or the highway") to the horribly complex ("would you like your friends whose birthdates are prime numbers to see your personal information?"). A different choice architecture (in particular, how defaults are defined) needs to be offered that makes it clear what the privacy options are and, even more importantly, what the consequences of your choice will be. It is one thing to agree to have a social network share your information with select advertisers, but quite another to find out that no one is accountable when the select advertisers have mishandled your data, which can now be exploited by scammers on the other side of the world to steal your identity.

The second is to create a compelling value framework for individual data, a topic addressed in Chapter 13 of this book. Beyond the definition and implementation details of this value framework, it is important to realize that the world of privacy is one that currently thrives on information asymmetry: companies that successfully exploit individual data understand the value of it while the individual has at best vague notions about it. Only when individuals understand the value of their personal data, and not just the bad things that can happen to them if it falls into the wrong hands, will they begin to take control of their personal information. As a driver of decisions, the promise of a short-term carrot always works better than the possibility

of a stick in the distant future; instead of letting this fact help advertisers promote $1 coupons for hamburgers in exchange for all your family's personal facts and figures, this should be leveraged to offer individuals value they can understand and control.

The third is to empower individuals to make informed choices about privacy. One of the most difficult tasks in this endeavor is to make it simple for the individual: there is no empowerment without ease of use. It is worth noting that making choices and consequences explicit and simpler is not just good for individuals but also for companies having to navigate an increasingly complex legal landscape around privacy: indeed, designing and implementing privacy policies is no less daunting a task in a world where network effects and cascading events produce hard-to-predict consequences.

I am not an expert on privacy but have spent most of the past decade studying choice and decision-making in complex, uncertain situations. Privacy strikes me as a perfect example. Below is an excerpt from a blog post I wrote for the Atlantic a few years back:

There is an intriguing parallel I want to expose in more detail between biological evolution and decision-making: search and evaluation in decision-making are similar to variation and selection in evolutionary theory. Search is all about creating a variety of options and possible answers to a query; evaluation is the process through which some or none of the options are selected. Nature thus provides us with a powerful metaphor for decision-making, and in that context genetic algorithms are decision-support tools. With interactive genetic algorithms, variation is performed by a non-human device while options generated by the device are evaluated by a human being.

In fact, we humans have been using this technique for hundreds of years, it is known under various names such as breeding, animal husbandry or directed evolution. To name one famous example, corn was bred about 9,000 years ago by Mexican farmers. Teosinte, the plant they started with, is so different from modern corn, that it was originally classified in a different genus. Teosinte is barely edible, while corn is today one of the leading sources of calories for humans.

The story of how such a transformation was made possible, by the combination of careful selection by farmers with a genetic structure that enabled dramatic morphological changes, is still being uncovered by ongoing research. Which means that humans have been using a powerful biological engine called variation which they did not understand at all; all they knew was that it worked for producing the requisite amount of variation and they could provide selective pressure.

The philosopher Daniel Dennett uses the phrase "competence without comprehension" to describe the strange value proposition of Darwinian evolution, that "to make a perfect and beautiful machine, it is not requisite to know how to make it" [MacKenzie RB. (Nisbet & Co., London, 1868), cited by Dennett]. Indeed, what McKenzie, a 19th-century critic of Darwin, calls "a strange inversion of reasoning" has been one of the weapons creationists have used.

But directed evolution is a highly successful embodiment of that inversion of reasoning—of competence without comprehension. Corn is the descendant through directed evolution of teosinte. The domestic dog, in its apparently infinite variety, is the product of many generations of breeding from just one common ancestor, the gray wolf. Examples abound.

In silico evolution, in the form of genetic algorithms, creates an opportunity for competence without [necessary] comprehension. You may be able to comprehend—either during or after the design process, but *you don't have to*. The machine takes care of the variation process. This is a powerful concept: think about all the situations in which you have to rely on an expert to produce variations for you—an architect, a designer, a brand naming consultant, etc. The expert is the gatekeeper between you and your dreams, and defines the possible on the basis of her own biases.

Your dreams are bounded by the expert. Yet you are an expert on knowing whether you like something or not. You may not understand how the expert comes up with the variations, but you're competent (in fact, you're likely the most competent) when it comes to your own tastes. Competence without comprehension empowers you to innovate far beyond your comprehension. One caveat is obviously that whatever new stuff you produce be safe.[7]

Privacy choices may be considered in a similar fashion. To wit, the average person will never be an expert in the many rules and requirements, some of which are discussed in this book. The average builder of systems or marketer of product or consumer of information similarly may never be an expert in the nearly infinite data points, information artifacts, and choices that may be made with regard to personal data or in the personal data economy.

A privacy component or privacy rules engine, however, may be developed to provide modeling or choice variants that can empower the most competent innovator to innovate far beyond her individual comprehension by providing reasonable and relevant choices that fit the criteria of the rules engine and enterprise objectives or desires. Similarly, the object of data processing (i.e., and the individual person who is described by personal data elements) may be able to choose from variants of privacy settings to optimize her selection to fit culture, taste, and general context without ever becoming an expert in the complexity that lies within.

These are some of the ways forward to address the conundrum of privacy. The objective is to strike a balance between the risks and rewards of personal information sharing, which requires a clear and explicit exposition of the risks and rewards. Contrary to what a certain social network executive stated, privacy is not a binary property rejected by the new social norms; the reality is so much more complex. And so much more fun.

[7] www.theatlantic.com/technology/archive/2011/03/how-evolution-helps-us-when-it-comes-to-making-decisions/72883/

Societal Pressures and Privacy

Social norms are always a part of the process when new technologies are being adopted by society. There are many examples of how technology has ushered in new changes that affect the way our world works. These changes must be accepted and adopted at a cultural level. Therefore, they typically occur in a wave-like fashion rather than as a disruptive event that happens overnight.

If we look at the Internet browser as an example, the initial concept created a disruption in the sense that it suddenly offered a new way to share information. Someone could publish data to a worldwide audience just by posting the data in one place. However, the implications of this have taken years to manifest and become part of our culture. The process has involved many twists and turns, including many unexpected effects on society, such as the current phenomenon that a person previously unknown in the public eye can become a virtual celebrity almost overnight after publishing information that goes viral.

Our society has now learned how to use the technology to make people's lives better. The first Mosaic browser was released to the public in 1993, but the idea of social networking was inconceivable at that time. It evolved after more than a decade of technology innovations[8] that eventually led to mass acceptance of Internet technologies. These technologies have provided a means to connect our global human race and have changed our society: We now can more easily connect to family and friends, get broad perspectives on specialized topics (like privacy), or learn of overseas disasters much more quickly; often we get the best insights from ordinary people who just happened to be at the scene at the time of a major event and chose to share their experience via social networking.

Social norms have no doubt shifted along the way and have affected the way we think about privacy. These social norms are different among different age groups. Some people have gone so far as to suggest that privacy is disappearing as a social norm in the younger generation and that they don't really care about keeping anything private. However, research evidence points to the contrary. There are clear generational differences about what constitutes privacy, but the younger generation still wants a world where they can share freely and yet have their privacy respected for the things that do matter to them.

> *And these children that you spit on, as they try to change their world, are immune to your consultations. They're quite aware of what they're going through.*
>
> —David Bowie, "Changes"

[8]Complex and convoluted technologies were a part of this evolution, but the graphical user interface is a prime example of outward simplicity and user centricity that took the Mosaic flash of brilliance to a worldwide revolution.

Recent research by danah boyd and Alice Marwick has shown that even though today's teens routinely use social networking to share information that many adults would consider private, they still care about their privacy on other fronts. The research found that teens want the ability to control their social situations and that it matters to them who is in their physical presence as well as who's watching when they are online or talking with friends. Like most of us, they act differently if they think they are being monitored. So, while they may not be concerned about sharing certain types of information, they do care about having control over their environment and about being able to exercise free will without concern about judgment or other consequences from parents or other authorities.[9]

If we look at history, we can see that our society has not only experienced shifting social norms over time but also has shown an incredible ability to adapt to change. The Industrial Revolution in the 19th century created sweeping changes that affected both social norms and economics. It enabled our society to build an educated workforce and a strong middle class. However, in that process our society had to learn how to balance the human needs of working-class citizens against corporate profit. Laborers formed unions to help make sure that the working class was not being taken advantage of by the elite. Society stood behind the notion that financial security should not be traded for a humane existence.

In today's information age, privacy has surfaced as a similar means by which the elite can in some ways take advantage of the masses. Humanity has a way of making sure that these imbalances don't last forever: We may not yet be able to see how balance will be restored in the area of privacy, but it is our belief that such a balance is virtually inevitable. Those individuals who embrace the need for privacy and bring innovations that help move humanity toward the balance we are seeking will likely find a surprisingly strong embrace by the general public and may be carried by a powerful new wave that ushers in the balance.

It's also important to think about what might happen to those who choose to ignore the call to action. As public awareness of privacy issues has grown, users expect organizations to be considerate of privacy rights. Management teams can no longer get away with big mistakes under the guise of naivety or ignorance: You're expected to be on top of privacy issues. Oversights will be seen as willful acts of betrayal or manifestations of gross incompetence that could quickly turn into bad press in addition to dissatisfied customers.

It Still Comes Down to Trust and Value

Although we may not know where technology will lead us, we do know that there is a central theme for users when it comes to privacy. At the end of the day, users want to do business with organizations they trust and where there is significant value. Can users trust your organization to safeguard their data? And do they see enough value in your product or service to want to hand over some personal data?

[9] "Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies," danah boyd and Alice Marwick, September 2011. www.danah.org/papers/2011/SocialPrivacyPLSC-Draft.pdf

Trust is built by respecting the user's right to privacy and by openly communicating as well as adhering to a coherent privacy policy. The fair use principles discussed in the early part of this book are just common sense. It's a matter of seeing things from the user's perspective and then putting some governance in place to make these principles an integral part of your organization and your product lifecycle.

Trust requires more than just doing the right thing: It's also about communication. If your communication is misleading or vague, it can create mistrust even though you may be technically doing what was said.

Trust can also be broken when we do something slightly different from what was communicated. An action that would fall within the fair-use principles but was not properly communicated to users can open the door for misinterpretation or mistrust.

Building trust also requires repeated behaviors over time. This is especially true if you're making changes to your privacy policy or how it is implemented. If there was reason to mistrust in the past, users may be reluctant to believe that your new approach represents a real change of heart. If you've adopted the privacy engineering principles espoused in this book, your privacy policy will be embedded in your products and services. However, it may take a full product cycle before your users recognize the change. If your organization can be consistent and transparent about treating PI with respect, the long run result will be a trusting user community and a positive public image.

A New Building Code for Privacy

Privacy is at an inflexion point. It has become a mainstream discipline, and organizations are beginning to take advantage of some of the old-school ways of engineering to build privacy into their products and build out their privacy vision. And yet, privacy engineering is more of an aspiration and a wish than a prolific practice in the face of massive collections of data and a greater ability to analyze, group, and decide based on these data artifacts. Many of the techniques spelled out in Part 2 of this book represent computer science disciplines that have been around for decades. These disciplines are being applied in new ways to leverage tried-and-true design principles while making privacy an integral part of product design.

History has shown that the best innovations are actually built on top of previously successful approaches. We believe that governance and evaluation models can and will evolve toward approaches that are both data centric and person centric. Today's product design reviews are still predominantly focused on protecting corporate interests; protecting privacy (a human right) rarely enters the conversation. To change this requires a new definition of corporate or organizational interests. Corporate interests must include not only building products to address market needs but also protecting users by protecting their data. A balanced approach would have equal focus on how to deliver value to the customer and how to protect the customer's right to privacy.

But how can we fulfill the human desire to be connected online in a way that does not feel like Big Brother is watching while also delivering value to the organization in which we work? It's complex and messy to attempt integrating these two vantage points. However, that doesn't mean we can't break down the complexity and use the techniques and best practices presented in this book to take the first steps toward the goal.

We may think we need a crystal-clear vision of the future of privacy in order to design for privacy, but if we look at nature and organic systems, we can find many examples

of things that are created out of orderly chaos. Flocks of birds, schools of fish, and ant colonies are all good examples of organic systems that create a beautiful and elegant result even though the individual participants don't really know the final result toward which they are headed. Organic systems follow simple rules that enable cooperation and steady progress toward a common goal. Each component of an organic system acts with consistency and integrity, and the components interact with one another in close proximity.

Organic systems also have a lifecycle. At some point, old plants die out and their seeds regenerate to form new plants. The human body expels or kills bad bacteria. Similarly, with our information systems, there is a need to either recycle or expel data that have reached the end of their lifecycle and become a potential risk. In the same way that computer viruses or malware can be detected and disabled to prevent damage, data that are no longer useful can be purged from the system to protect personal privacy. Many organizations tend to hoard data while attempting to find ways to derive value from them. If there is no clear use for the data, then they are simply a threat and it's best to properly dispose of them.

If we believe that our customers want to buy from organizations that not only offer valuable products and services but also are respectful of user rights and provide transparency, then we have our design principles. Personal information can be treated as a living entity that must be shared or stored in ways that preserve integrity and enable an elegant outcome. Perhaps there are innovative ways to give users more choice about when their data are saved and for how long. Data retention rules could then be different for different users and yet be implemented automatically with great efficiency.

We can build great products around these lofty goals without knowing how the future of privacy will look a decade from now. Innovation requires taking action from where we are today. Perhaps we can even design systems in which there are frequent interactions between data elements and system or machine components. This can let the system itself determine if there is value in continuing to maintain and store the data. If we've modeled our data well, we will know the places and times in the lifecycle where the data have value. Then we can automate the movement of data through the lifecycle in a way that preserves value and minimizes risk.

Meeting user needs for privacy in new and innovative ways will allow you to be part of a revolution that may help to bring humanity back into balance.

Getting Started

Now is the time to decide your direction regarding the building blocks that you will create for constructing your privacy foundation. Your building blocks will be based on an overall approach to privacy and will determine how PI is treated within your products or services. The approach must be determined first because it could be difficult to change course after implementing parts of your privacy vision. Think about how difficult it would be for Facebook to change their privacy orientation now that users have become accustomed to the free sharing of information that is promoted in the current environment.

Once your overall approach and orientation are defined, it should be easy to determine what steps to take next because you'll notice areas that are not well aligned with your new approach. You may notice both new opportunities and unchecked risks. To get started, you'll need to take stock of where you are today. By surveying the situation, you can identify areas that need immediate attention and also envision new long-term opportunities. It's not necessary to have a complete long-term plan to begin taking action. The important thing is that action can be taken from where you are today. In many cases, it's possible to identify short-term goals and get the ball rolling in the right direction. A more comprehensive planning process can be concurrent with addressing some of the short-term needs.

The following are examples of some of the actions that may be good starting points once you've surveyed your situation:

- Build consensus among functional organizations regarding how privacy requirements can become part of your overall process for defining product requirements
- Add privacy as a component of your organization's ethics
- Decide to adopt some of the structured approaches for product development that are defined in Part 2 of this book
- Modify your governance processes
- Train your engineers so they know what their options are
- Create organizational incentives for privacy so that privacy gets baked into product design and other parts of the product lifecycle

Whatever course you choose, it's important to be mindful of fair-use principles and the inherent value of data as you move forward on your course to embed privacy principles into all phases of your product lifecycle.

A Privacy Engineer's Manifesto

We'd like to leave you with a manifesto that provides some guiding principles for you as a privacy engineer. These principles are an attempt to illuminate a belief system in which the seemingly opposing motives of creating corporate profit and respecting individual privacy can live in harmony. Here you may find a meeting grounds that enables both your organization and your customers to profit—each in their own ways.

1. ***Data about people is valuable in and of itself.***

   Data provide commercial value to businesses in addition to their inherent value from a personal perspective. They also provide value as an exchange or a unique identifier to build social connections. A privacy engineer understands this principle as bedrock and strives to find innovative ways to extend the value of data while protecting their inherent value.

2. ***A privacy engineer needs more than just technical skills to protect and extend the value of data.***

   The inherent value of data that is attained from or attributable to human beings requires a number of different perspectives and skill sets to be effective. The privacy engineer, as a modern renaissance type discipline, views personal data through legal, creative, and personal lenses.

3. ***A privacy engineer draws from artistic creativity and expression to innovate and communicate.***

   Beyond learning from sister disciplines to add to the known world of technology, the privacy engineer seeks to create simplicity, clarity, and beauty to engage and inform users and owners of systems. The tools of engagement can use sound, taste, touch, sight, smell, intuition, or any other artistic medium. Technologies, policies, laws, organization, and metric modalities all have interfaces. Effective interfaces can be engaging, challenging, educational, elegant, emotive, and even beautiful where innovation meets art.

4. ***A privacy engineer learns from, but disregards, the failures of the past.***

   While building on past successes as well as the remnants of previous attempts at success, a privacy engineer closely regards and incorporates existing tools, policies, and frameworks as scaffolding to create something wonderful. (Borrowed heavily from Intel founder Bob Noyes.) A privacy engineer strives to map and develop data systems in a scientific fashion in order to create new or improved means of delivering value to all parties who have a vested interest in the data.

5. ***We are all privacy engineers.***

   We all possess or are the subject of PI and have a vested interest in protecting it. Some of us have occasion to operate as "professional privacy engineers," but all of us at least operate as "citizen privacy engineers" when we act as stewards of our own PI and the PI of others.

6. ***For the privacy engineer, with the mantra to innovate comes the mantra to do no harm.***

   The privacy engineer's goal should be to harness the inherent value of data and innovate to create additional value. But the most basic requirement for the privacy engineer is to do no harm and to plan to eliminate as much secondary or unanticipated harm as possible.

7. ***Innovation and complexity need not be the adversary of privacy engineering, although failure of imagination may be.***

   What is not thought of cannot be recognized and therefore cannot be managed. Failures of imagination are thus the biggest enemy of the privacy engineer. Failure to imagine a new possibility means that a value creating opportunity or a risk mitigation opportunity has been missed.

8. ***The privacy engineer must be able to understand, calculate, mitigate, and accept risk.***

   The privacy engineer cannot ignore risk or fall prey to the idea that it can be completely eliminated. By embracing both risk and value, the privacy engineer can strive to find solutions that deliver maximum value at an acceptable risk level to the organization and the individual.

9. ***Privacy engineering happens inside and outside of code.***

   Coding, building systems, and the business processes that support the product lifecycle are critical. A foundation of privacy principles and operational business processes can support development of products that promote privacy. At the same time, the individual doing the developing may see opportunities for innovation that can only be envisioned by one who is at the proverbial drawing board.

10. ***A privacy engineer needs to differentiate between bad ideas and bad implementations.***

    A *bad idea* is one that goes against privacy principles or lacks sound judgment about using and protecting PI. A *bad implementation* is when the design goal is sound but the implementation is not due to poor usability, unmitigated risks, or an approach that weakens the bond of trust with users. In the latter scenario, a bad implementation that may harm data privacy may be rearchitected or protected in another layered fashion, whereas, in the former, a bad idea should be acknowledged and quickly ended before damage is done.

Conclusion

If you've taken the time to read this book, you've already made a commitment to be a change agent in the field of privacy. Our hope is that we've presented some new ideas for you and that you'll use these ideas to help make the world a better place.

We've done our best to lay out some concrete steps that you can adopt today while your future vision continues to evolve over time. Taken to heart, the principles in the manifesto can both shape your future vision and guide your daily activities.

May you achieve success by innovating in ways that align with the trends already shaping our shared world. The future we inhabit together is being shaped by the big and small decisions that each of us make daily.

Go forth and innovate!

Often when you think you're at the end of something, you're at the beginning of something else.

—Mister Rogers