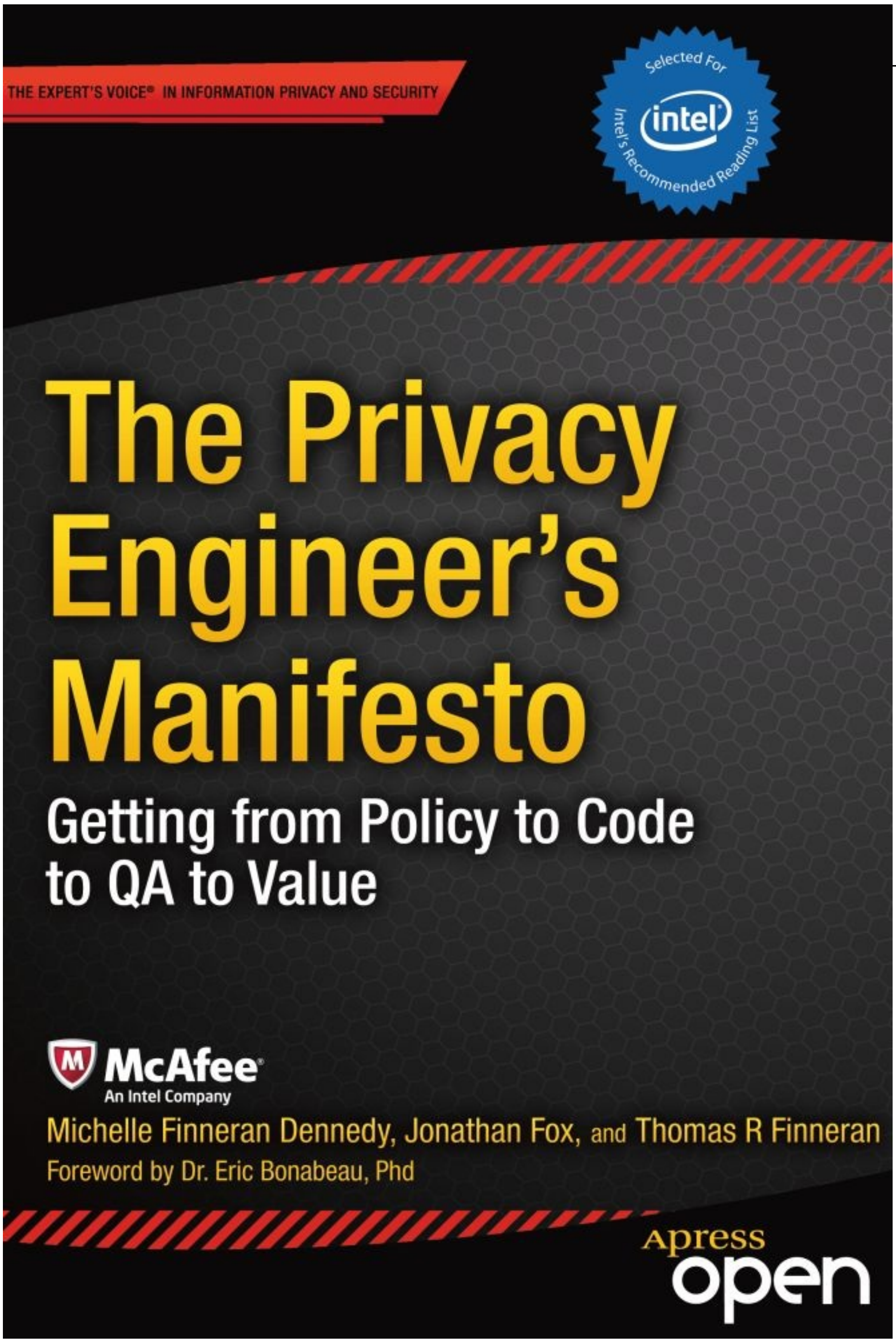


THE EXPERT'S VOICE® IN INFORMATION PRIVACY AND SECURITY

Selected For intel® Intel's Recommended Reading List

The Privacy Engineer's Manifesto

Getting from Policy to Code to QA to Value

McAfee® An Intel Company

Michelle Finneran Dennedy, Jonathan Fox, and Thomas R Finneran

Foreword by Dr. Eric Bonabeau, Phd

Apress open

Michelle Finneran Dennedy, Jonathan Fox and Thomas R. Finneran, *The Privacy Engineer's Manifesto*, Getting from Policy to Cod
to QA to Value, DOI: 10.1007/978-1-4302-6356-2, © Apress 2014

Michelle Finneran Dennedy, Jonathan Fox and Thomas R. Finneran

The Privacy Engineer's Manifesto

Getting from Policy to Code to QA to Value

Selected For intel Intel's Recommended Reading List

Apress

Michelle Finneran Dennedy

Jonathan Fox

Thomas R. Finneran

ISBN 978-1-4302-6355-5 e-ISBN 978-1-4302-6356-2

© Apress 2014

The Privacy Engineer’s Manifesto

Michelle Finneran Dennedy, Jonathan Fox, and Thomas R Finneran

ApressOpen Rights: You have the right to copy, use, and distribute this Work in its entirety, electronically without modification, for non-commercial purposes only. However, you have the additional right to use or alter any source code in this Work for any commercial or non-commercial purpose which must be accompanied by the licenses in (2) and (3) below to distribute the source cod for instances of greater than 5 lines of code. Licenses (1), (2), and (3) below and the intervening text must be provided in any use of the text of the Work and fully describes the license granted herein to the Work.

(1) **License for Distribution of the Work:** This Work is copyrighted by Apress Media, LLC, all rights reserved. Use of this Work other than as provided for in this license is prohibited. By exercisir any of the rights herein, you are accepting the terms of this license. You have the non-exclusive right to copy, use, and distribute this English language Work in its entirety, electronically without modification except for those modifications necessary for formatting on specific devices, for all non-commercial purposes, in all media and formats known now or hereafter. While the advice and information in this Work are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to th material contained herein.

If your distribution is solely Apress source code or uses Apress source code intact, the following licenses (2) and (3) must accompany the source code. If your use is an adaptation of the source code provided by Apress in this Work, then you must use only license (3).

(2) **License for Direct Reproduction of Apress Source Code:** This source code, from ***TouchDevelop: Programming on the Go, ISBN 978-1-4302-6136-0*** is copyrighted by Apress Media, LLC, all rights reserved. Any direct reproduction of this Apress source code is permitted but must contain this license. The following license must be provided for any use of the source code from this product of greater than 5 lines wherein the code is adapted or altered from its original Apress form. This Apress code is presented AS IS and Apress makes no claims to, representations, or warrantees a to the function, usability, accuracy, or usefulness of this code.

(3) **License for Distribution of Adaptation of Apress Source Code:** Portions of the source code provided are used or adapted from ***TouchDevelop: Programming on the Go, ISBN 978-1-4302-6136-0*** copyright Apress Media LLC. Any use or reuse of this Apress source code must contain this Licens This Apress code is made available at `Apress.com/978143026136-0` as is and Apress makes no claims

to, representations, or warrantees as to the function, usability, accuracy, or usefulness of this code.

~~President and Publisher: Paul Manning~~
Lead Editor: Steve Weiss
Technical Reviewers: Richard Schaefer and Stuart Tyler
Coordinating Editor: Jill Balzano
Copy Editor: Mary Bearden
Cover Designer: Anna Ishchenko

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail `orders-ny@springer-sbm.com`, or visit `www.springeronline.com` .

For information on translations, please e-mail `rights@apress.com`, or visit `www.apress.com` .

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinio as to whether or not they are subject to proprietary rights.While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editor nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

To ~~our children, our families, and privacy engineers everywhere—past, present, and future.~~

Foreword, with the Zeal of a Convert

It’s a call I get every 6 to 12 months. My credit card has been “compromised” and needs to be replaced with a new one. Once a major annoyance, this has become a well-oiled, mildly inconvenient ritual for updating useful accounts and dropping the ones I no longer need or want—an effective method for canceling sticky subscriptions. It is a tribute to the resilience of human beings that we can adapt so easily to a bad state of affairs. And so it is for me, and many others I suspect, the way that I am reminded about privacy and its protection, by accident, every 6 to 12 months, for just a few days. It’s not that I don’t like privacy; it’s just that I really didn’t care all that much.

The book you are holding at this instant is what made me care, deeply. It didn’t happen for ideological reasons, nor because I favor anonymity, although I do like it, at times of my choosing. No I care because the “privacy engineering” framework, methods, and processes the authors have put together are critical enablers to unlock value from data. However strange that may sound (after all, isn’t privacy all about preventing companies from gaining access to customer data?), it makes sense when you consider the complexity of dealing in practice with the absurd amounts of data individuals, companies, and governments are producing and accumulating at an accelerating pace. The keyword here is complexity. Having spent the past two decades studying and modeling complex systems, I am not the most unbiased of observers, but, given that we all have our biases, I hope you will find mine useful.[1] I tend to view the most interesting problems through the lens of complex systems, and data, particularly in large quantity, strike me as a complex system of sorts.

Data as a Complex, Evolving, Self-Organizing System

Let’s consider, for the purpose of this Foreword, data about individuals—their attributes and behaviors as they have been captured digitally, with or without consent from the individuals, often redundantly and with errors. All those data about one single individual constitute a mini-ecosystem, a mini-PIE (personal information ecosystem). The mini-PIE is populated with many interacting specie when a ZIP code interacts with a list of recently visited web pages, an (allegedly relevant) advertisement may be created, the response to which will be added to the mini-PIE. When a misspelled version of a name interacts with a web site account, it results in a rejection; but when the same misspelled version of a name interacts with a Department of Homeland Security database, it may wreak havoc in the individual’s life.

Each time there is an interaction, it adds richness and complexity to the mini-PIE. Your very own mini-PIE, which is in fact your digital identity, exhibits many coexisting dynamical patterns of behavior: you pay your bills on time, you travel domestically about three times per month and overseas twice a year, you visit 57 news sources on average in a given week, you purchase a lot of items on Amazon around December 18, and, to play on the infamous Target-knows-everything example, your daughter’s buying patterns suggest she is pregnant even though you don’t know (yet). The truth is, there are millions, even billions of possible patterns in your mini-PIE: yes, your PIE can be sliced in that many ways.

Now consider bringing together the mini-PIEs of thousands or even millions of individuals, a typical number for, say, a midsize retailer. All these interacting species can now interact between individuals, not just within one individual’s mini-PIE. Some of these interactions are implicit: “my ZIP code is the same as your ZIP code,” while others are explicit: “my (pregnant?) daughter is Facebook friends with your (suspicious?) son.” The interacting species from all the mini-PIEs form a big PIE covering many individuals, with each species a building block that can be combined in many different ways to address many different questions. The trouble is, the number of possible ~~combinations is, well, combinatorial, which means that it increases faster than exponentially wi~~th the number of building blocks and therefore the number of individuals in the PIE, a concept we will encounter again soon. I hope to have convinced you, however imperfectly, that personal information a complex system. Now is a good time to examine the consequences.

Complexity

The problem with increasing the number of interacting building blocks in a PIE is that finding the right combinations becomes a quixotic task. If you are looking for correlations in the data, which seems to be the new scientific method, the number of spurious correlations increases much faster tha their more meaningful counterparts. In *Antifragile*, economist and author Nassim Taleb sums it up: “in large data sets, large deviations are vastly more attributable to noise (or variance) than to information (or signal).”[2] He adds, “falsity grows faster than information.” In other words, we can expect many correlations that are statistically significant but ultimately meaningless. It follows that order to exploit the complexity inherent in very large datasets, you need a way to weed out most of th meaningless correlations that inevitably show up all over the place.

Emergence

In addition to the combinatorial complexity of putting together the right building blocks, there is the delicious problem of emergence: the whole is more (or less) than the sum of its parts (building blocks), meaning that you cannot know ahead of time what a combination of building blocks will produce. Put two or three innocuous building blocks together and the result might be equally innocuous—or spectacularly interesting. To use a national security example, let’s assume that the three building blocks are as follows: (1) Suspicious individuals are learning to fly aircraft without learning how to land. (2) Web site chatter indicates that a terrorist event will take place on 9/11. (3) suspected terrorist told his friends in a chat room that there will soon be an attack against the World Trade Center in New York. I wouldn’t call any of these building blocks innocuous, so they are not, individually, actionable. However, if you know to put them together, you get a very actionable piece of intelligence. Of course, I am assuming here that you know to put these three particular building blocks together, but the main point is that the value of the combination is much, much greater than th sum of the individual building block’s value. This type of emergence is ubiquitous in PIEs. Just as th combination of unclassified individual parts can produce classified information, the combination of perfectly legal parts can be illegal. Another kind of emergent phenomenon happens when building blocks are plunged into a new environment, revealing previously concealed properties: for example, combination of building blocks that is legal to store in one country could become illegal the minute you cross a border, reflecting a change in the legal environment. That makes the calculus of privacy tricky.

Self-Organization

Some of the more interesting emergent patterns that can be observed in PIEs are patterns of self-organization. It is an interesting property of ecosystems that species interact with one another, thereb modifying their environment, which in turn changes the way they interact with other species. To see how the concept applies here, let’s consider the very, very big Amazon PIE. Amazon customers leave data trails similar to the pheromone trails of ants: the more pheromone on a trail, the more ants are ~~attracted to the trail, further reinforcing the trail’s pheromone concentration, a well-known example~~ o self-organization in biological systems. The net result for Amazon customers is well-groomed trails t the most popular products as these products attract more reviews, which makes other customers more comfortable and gives Amazon an incentive to promote them since these products sell more easily.

Recommender systems seem largely stuck in the collaborative filtering model, an inherently self-reinforcing method corralling the masses toward self-defining blockbusters and away from the “long tail,” those products that sell just a few pieces every year. Collaborative filtering does not rely on you personal characteristics but rather on a generic set of PIE building blocks: the overlap between what you have purchased and what other people have purchased. Beyond recommender systems, you will find a similar kind of self-reinforcing dynamics in every situation where a certain type of building block from your PIE will be used to increase its own importance. For example, if you are a frequent traveler on an airline, you can very easily become a “known traveler” and peruse the keep-your-shoes-on-and-your-laptop-in-the-bag security line at the airport, a perk that increases the likelihood that yo will continue to pile up the miles with that airline. What is missing in this picture is creativity and innovation. Even ants sometimes wander off their columns and get lost when finding new food sources, and so must data-mining algorithms, or we will be stuck on boring, self-reinforcing highway for a long time, ignoring other opportunities. One example of a company that should give us hope use evolution as its creativity engine. Its name? Pandora.

Evolution

Pandora has identified the building blocks of music and musical tastes. A team of experienced musicologists have painstakingly analyzed tens of thousands of songs spanning all musical genres using a set of 450 well-defined attributes that characterize the music and listeners’ musical preferences. Pandora calls this treasure trove of precise taxonomic information the Music Genome Project (MGP), a key asset that has made the company a beloved personalized radio station: discover is not based on what others like but on what you like. Pandora asks a listener to rate multiple songs and uses its MGP to evolve and mutate the genomes of the preferred songs to discover songs that might be of interest to that particular listener. A common experience with Pandora is to discover an artist or song that you love but had no idea even existed: you wouldn’t have been able to search for it but you know it is a great match in the first seconds of hearing it. In other words, Pandora provides a example of evolutionary dynamics in a mini-PIE. But for this to work, “the MGP’s database is built using a methodology that includes the use of precisely defined terminology, a consistent frame of reference, redundant analysis, and ongoing quality control to ensure that data integrity remains reliably high.”[3] Similarly, if we are to discover not just songs but more general patterns in data, the underlying data need to have the same characteristics as the Pandora MGP data.

As dean of a College of Computational Sciences, focused on critical analysis and creative thinking, I have established “Know thy data” as one of the core learning objectives of our curriculum Well, it’s expressed in less memorable terms: “Consider the nature, scope, quality, sampling, origin and context of the data, including the existence of a control group.” In other words, the integrity and traceability of data are crucial to what you can do with it, a core theme of privacy engineering. Modelers have a well-known expression: garbage in, garbage out. Problem is, you don’t know for sur that it’s garbage if you haven’t prepared your data properly.

Once the underlying data structure is in place and all methods and processes are properly implemented, amazing things become possible if you view data as the genetic code of value propositions. In the case of the Pandora value proposition, it is literally true. But it is generally true that data building blocks are combined, mutated, and recombined to create new value propositions. ~~Innovation comes from combining and reconfiguring existing building blocks differently.~~ Consider Capital One, the credit card company that invented balance transfer and is famous for experimenting at scale by creating and sending out tailored offers to potential customers, waiting for results to come in, and then modifying its offers in response to the profitability of a particular combination of offer and segment. The continuous feedback, although it was taking place on a longer timescale than Pandora’s, is of the same nature, with the data building blocks defining [offer] × [segment] being mutated and recombined in response to customer behavior. The same principle is widely applicable, from the mundane A/B testing used by savvy Internet companies to the design of entire business strategies. But before anything can be done, you need a privacy engineering strategy.

Foreword’s Epilogue

“My company has been collecting a megaton of data over the years and we have used it for reporting but we think there is value in it that we’re not exploiting. But we don’t know where and how to look. Help us discover the value in it.” In just one year, this kind of statement has become commonplace in my conversations with executives all over the world. Privacy is rarely mentioned, and even then, only as a hindrance. Let me note in passing that privacy, as a field, should probably be renamed. There is no sense of urgency or value in the word privacy, a problem that has plagued the field and will one da be addressed by shrewd marketers. Therein lies the beauty of privacy engineering: not only do data that have been “privacy engineered” comply with rules and regulations, they are also ready for exploitation, thereby transforming a legal burden into an opportunity for value creation.

Just as a prelude, consider what privacy engineering can do to clinical trials in the drug development process. The future of clinical trials is the quasi-disappearance of clinical trials: they ar slow, large, expensive, indiscriminate, and produce flawed results—they need to go in their current incarnation. The most promising alternative approach is based on “real-world outcomes,” that is, observational studies that do not rely on the randomized controlled trial (RCT) concept. Powerful statistical techniques can to a large extent “replicate” RCTs and establish causation. With this approach, the same data building blocks (age, race, gender, genotypic attributes, lifestyle attributes, drugs used, etc.) can be used, reused, and recombined multiple times depending on the question being studied, lowering drastically the cost and duration of studies and boosting innovation. But for that approach to be possible, well, the building blocks need to be legal, and dependable and their integrity ensured. In other words, the data have to be privacy engineered.

As for that credit card call, if the appropriate data building blocks had been kept separate, I wouldn’t have received it. But it’s become my best strategy to get out of sticky subscriptions.

Dr. Eric Bonabeau, PhD

About ApressOpen

What Is ApressOpen?

- ApressOpen is an open access book program that publishes high-quality technical and business information.
- ApressOpen eBooks are available for global, free, noncommercial use.
- ApressOpen eBooks are available in PDF, ePub, and Mobi formats.
- The user friendly ApressOpen free eBook license is presented on the copyright page of this book
- Interested in sponsoring a book on the ApressOpen platform? Please contact us at `apressopem@apress.com`.

About the Authors

Michelle Finneran Dennedy

VP, Chief Privacy Officer, McAfee

Michelle currently serves as McAfee’s Chief Privacy Officer where she is responsible for the development and implementation of McAfee’s data privacy policies and practices, working across business groups to drive data privacy excellence across the security continuum. Before coming to McAfee, Michelle founded The iDennedy Project, a public service organization to address privacy needs in sensitive populations, such as children and the elderly, and emerging technology paradigms. Michelle is also a founder and editor in chief of a new media site— `theIdentityProject.com` —that was started as an advocacy and education site, currently focused on the growing crime of Child ID theft.

Michelle was the Vice President for Security & Privacy Solutions for the Oracle Corporation. Before the Oracle acquisition of Sun, Michelle was Chief Data Governance Officer within the Cloud Computing division at Sun Microsystems, Inc. Michelle also served as Sun’s Chief Privacy Officer.

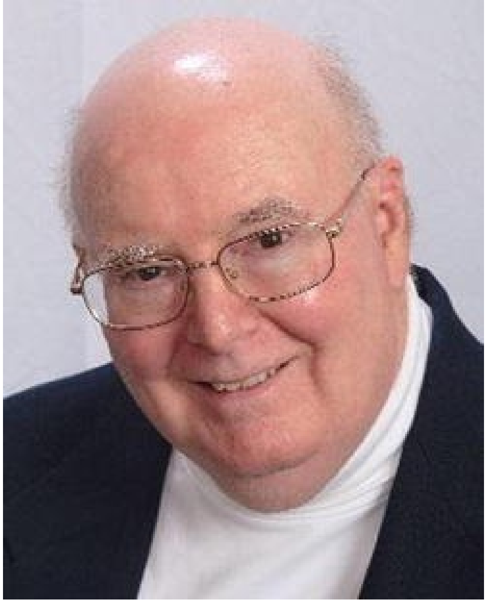
Michelle has a JD from Fordham University School of Law and a BS degree with university honors from The Ohio State University. In 2009, she was awarded the Goodwin Procter-IAPP Vanguard award for lifetime achievement and the EWF – CSO Magazine Woman of Influence award for work in the privacy and security fields. In 2012, she was recognized by the National Diversity Council as one of California’s Most Powerful & Influential Women.

Jonathan Fox is the global director of data privacy at McAfee.

Previous to McAfee, he was the worldwide director of privacy at eBay Inc., and before that, deputy chief privacy officer at Sun Microsystems, Inc. He has worked closely with marketing, information security, engineering, internal audit, professional services, technical support, and cloud teams to establish policies and operate programs to ensure the protection of customer and employee personal information. He is a certified information privacy professional (CIPP/US), a certified information privacy manager (CIPM), and was a certified information security manager (CISM). He is on the International Association of Privacy Professional's certification advisory board. His prior roles have included editor-in-chief of sun.com, business development manager for a new media startup, senior manager of electronic and intellectual property licensing for Random House, and program delivery manager for the Oracle Developer's Programme. He is a graduate of Columbia University. He regularly speaks at industry events on privacy issues.

His writing credits include:

- THE CIO AND THE CPO – A VISION FOR TEAMWORK AND SUCCESS, Sun Microsystems, 2006
- ESTABLISHING A PRIVACY OFFICE, Sun Microsystems, 2007
- PRIVACY IN THE PARTICIPATION AGE, Sun Microsystems, Inc., 2008



Thomas R. Finneran is a principal consultant for the IDennedy

Project. He has proposed an approach to use the Organization for the Advancement of Structured ~~Information Standards (OASIS) UML Standard for privacy analysis. He was a consultant for over~~ 25 years for CIBER, Inc. He has acquired over 25 years of experience in the field of information technology. His strengths include enterprise (including data, information, knowledge, business, and application) architecture, business and data analysis, UML object analysis and design, logical data modeling, database systems design and analysis, information resource management methodologies, CASE and metadata repository tools, project management, and computer law. He is experienced in almost all application system areas, including real-time data collection systems, inventory control, sales and order processing, personnel, all types of financial systems, the use of expert systems, and project management systems. He has developed and taught training courses in the areas of use cases, relational concepts, strategic data planning, logical data modeling, and the utilization of CASE tools, among others. He is also an experienced intellectual property patent lawyer. For various companies, he has held such titles as director, MIS; manager, corporate data strategy; manager, data administration; managing consultant; manager, standards and education; and systems designer. These companies include the Standard Oil Company, Corning Glass Works, ITT, ADR, and the U.S. Navy. I addition, he was vice president and general counsel of TOMARK, Inc., the developer of the highly successful ABEND-AID software package. He has a bachelor of arts (Ohio State University), a master's of business administration (Roosevelt University), and a juris doctor's degree (Cleveland State). He is a member of the bar of the U.S. Supreme Court and a member of the bar of Ohio, New Jersey, Connecticut and a member of the Patent Bar. His published papers include:

Enterprise Architecture: What and Why (www.tdan.com/i007ht03.htm);

Enterprise Architecture: The What's and How's (www.tdan.com/i018ht02.htm);

A Component-Based Knowledge Management System (www.tdan.com/i009hy04.htm);

A Best Practices Assessment (www.tdan.com/i012ht04.htm); E-Biz Metrics (www.tdan.com/i014hy03.htm);

Doing .Net Right: Looking at the Critical Success Factors (www.tdan.come /i020hy04.htm);

"Data Deliverables", Database Management (Auerbach Press) (1990);

"Business Analysis for Database Design" (Datamation, Nov. 1977)

About the Technical Reviewers

Richard Schaefer is the director of technical alliances at Good Technology. He is responsible for all aspects of ISV integration with Good’s secure mobility platform including security compliance. His longtime career focus is market adoption of evolutionary technologies primarily via partner ecosystems. His roles have spanned engineering, marketing, and business development in the application of nascent computing platforms and processes to a broad range of industries. His achievements have earned him awards and executive recognition at Sun Microsystems and Good. He has edited and contributed to books on the Solaris operating system, multithreading, and Java. Michelle Finneran Dennedy frequently introduces him as the one who taugh her about garbage collection.

Stuart Tyler is a senior privacy analyst at Intel Corporation with more than 13 years of hands-on privacy experience gained in Europe and the United States, covering every conceivable aspect of privacy including operational compliance, product and service development, and external public policy.

Introduction

The world is ***certainly*** flat. Everyone said so. The government said so. The Church said so. Your wise old aunt and the richest guy in town said so. **Everyone**.

Except, a few explorers and dreamers and scientists and artists and plainspoken folks looked out a a sky that appeared more like a bowl and noticed that the ground and sky always met for a brief kiss before the observer wandered ever closer and the meeting became elusive once more. And shadows and tides and other indications seemed to suggest that there might be something more than dragons beyond the edge of the world. And so, as it turned out, the world was not, in fact flat. There was a seemingly endless set of new possibilities to discover.

Privacy is ***certainly*** dead. Everyone said so. Rich people with big boats who sold stuff to the CIA in the 1970s said so. Founders of important hardware companies said so. Someone who blogs said so The government cannot make up its mind which person should say so or if the polling numbers look right, but it might say so. Someone tweeted. Even really old technologists who helped invent the whole thing said so. **Everyone**.

Except, a few explorers and inventors and philosophers and children and parents and even government regulators looked out at a seemingly endless sea of data and still can see how a person ca be distinguished from a pile of metadata. And people who wish to decide for themselves the story tha they wish to tell about themselves and to whom see a different horizon. The privacy engineer sees thi horizon where privacy and security combine to create value as a similarly challenging and exciting time for exploration, innovation and creation; not defeat. There are a seemingly endless set of new possibilities to discover.

The purpose of this book is to provide, a systematic engineering approach to develop privacy policies based upon enterprise goals and appropriate government regulations. Privacy procedures, standards, guidelines, policies and mechanisms can then be designed and implemented. A systems-engineering set of methodologies, models, and patterns that are well known and well regarded but are also presented in a creative way are used as models to guide the privacy engineer along on their journey. A proposed quality-assurance-checklist methodology and possible value models are described. But why bother?

The debate about data privacy, ownership, and reputation pose an irresistible and largely intractable set of questions. Since the beginning of recorded history, people have sought connection, culture, and commerce resulting from sharing aspects about themselves with others. New means of communication, travel, business, and every other social combination continue to evolve to drive greater and greater opportunities for the solo self to be expressed and to express oneself in person an remotely. It is all terribly exciting. Yet, every individual still desires a sense of individuality and space from his fellow man; a right to be let alone without undue interference to lead his individual life.

Governments have played a stark role in the development of data privacy. Laws are created to protect. But laws are also drawn in reaction to abuses and challenges to individual rights and freedoms. To futher complicate matters, laws are created in an unharmonized, multicultural context betwixt and between multiple governments in a world where people have become free to travel with relative ease and comfort—sans peanuts—around the globe and back again. National and internationa security norms have been challenged in both heroic and embarrassing fits and starts. The role of Tota Information versus insight and actionable information is debated again and again. “Insiders” and fam seekers have exposed massive data collection programs.

In the information technology sector, data privacy remains a matter for heated debate. At times th debate seems as if technologists somehow wish (or believe) they could escape the norms of general soc~~ial, cultural, and legal discourse. Simply by designing ever-more complex systems and protoc~~ols that "need" increasing levels of sensitive information to work, technologists' actions (or creations) seem to deny the basic requirement to respect data about people. Lawyers have come trooping in en masse to write similarly complex terms and conditions and hope to paper over the problem or find a cozy loophole in unholy legislative agendas. Investors search in vain for beans to count. Everyone els finds privacy booooooooorrrrring… until their own self interests are compromised.

Just as automotive technology eventually became a ubiquitous and necessary part of many more lives, so too has information technology from PCs to phones to "the cloud" become an essential part of industrialized nation states' economic stability and cultural expectations. Personal data fuels and preserves the value of this new information boom. The time has come where the elite can no longer dismiss the debate or pretend that data privacy doesn't matter. Our society cannot continue to build new creations that defy basic privacy precepts (that we will discuss herein) if they wish to see this ne world unfold and grow to its true potential.

If an executive at a global company publicly stated that he just doesn't *believe* in taxes and therefore will *simply not pay them* to any government, he would likely be removed or at least considered to be a great humorist. Not so for data privacy in the past. In the past decades, executives and other makers and consumers of information technologies regarded data privacy as some sort of religion that they could believe in--or not--at will and without consequence. They certainly did not regard privacy as a *requirement* to measure, to debate in the boardroom, or to build at the workbench We see these uninformed days of privacy as religion as nearly over. The age of data privacy as a set o design objects, requirements for engineering, and quality measures is dawning and we hope to help th sun to come shining in. There are possibilities, not dragons, over the new horizon.

In fact, we believe that plain-old-fashioned greed and an instinct for value creation will actually hasten the age of privacy engineering and quality. We know that the concept of privacy regarding one's person, one's reputation, and, ultimately, what can be known about the person, has been the inspiration of law and policy; but we also know that innovation has real value, and we know that privacy—informational or physical—holds the same.

Andrew Grove, co-founder and former CEO of Intel Corporation, offered his thoughts on internet privacy in an interview in 2000[4]:

"Privacy is one of the biggest problems in this new electronic age. At the heart of the Internet culture is a force that wants to find out everything about you. And once it has found out everything about you and two hundred million others, that's a very valuable asset, and people will be tempted to trade and do commerce with that asset. This wasn't the information that people were thinking of wher they called this the information age."

Thus, people living in the Information Age are faced with a conundrum: They wish to be connected on a series of global, interconnected networks. But, they also want to protect their privacy and to be left alone…sometimes. Both business and governmental enterprises, striving to provide a broad base of services to their user community, must ensure that personal information and confidential data related to it are protected. Those who create those systems with elegance, efficienc and measurable components will profit and proliferate. History is on our side.

We call the book and our approach "Privacy Engineering" in recognition that the techniques used to design and build other types of purposefully architected systems can and should be deployed to build or repair systems that manage data related to human beings.

We could have similarly called the book "Design Principles for Privacy", because the techniques and inspirations embraced by the Design communities in informatics, critical design and, of course, systems design are also a part of the basic premise where one can review an existing successful framework or standard and find inspiration and structure for building and innovation. The very ~~nomenclature of "Privacy Engineering" is left open to the possibility of further design.~~

The models shown in this book are abstractions. Models are never the reality, but models and patterns help designers, stakeholders, and developers to better understand and communicate required reality.

Confidence in privacy protection will encourage trust that information collected from system use will be used correctly. This confidence will encourage investment in the enterprise and, in the case o charity enterprises, will encourage people to donate.

There are many books and papers on privacy. Some focus upon privacy law, others focus on general privacy concepts. Some explain organizational or management techniques. This book is intended to be additive. This book crosses the boundaries of law, hardware design, software, architecture, and design (critical, aesthetic and functional). This book challenges and teases philosophical debates but does not purport to solve nor dissolve any of them. It discusses how to develop good functionalized privacy policies, and it shows recognized methodologies and modeling approaches adapted to solving privacy problems. We introduce creative privacy models and design approaches that are not technology-specific nor jurisdiction-specific. Our approach is adaptable to various technologies in various jurisdictions.

Simply put, this is a book of TinkerToy[5] like components for those who would tinker, design, innovate, and create systems and functional interfaces that enhance data privacy with a sustainability that invites transparency and further innovation. We wish to demystify privacy laws and regulations and nuanced privacy concepts into concrete things that can be configured with flexible, engineered solutions.

The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value is a unique book. We introduce privacy engineering as a discrete discipline or field of inquiry; innovation may be defined as using engineering principles and techniques to build controls and measures into processes systems, components, and products that enable the authorized processing of personal information. W take you through developing privacy policy, then to system design and implementation, to QA testin and privacy impact assessment, and finally (actually, all throughout the book) discussions about valu

- Chapter 1 introduces the evolution of information technology and the network, and its impact o privacy.
- In chapter 2, we discuss a series of definitions: policy, privacy engineering, personal informatio (PI), and the Fair Information Processing Principles (FIPPS).
- Chapter 3 covers d*ata and privacy governance*, including *data governance*, *Generally Accepted Privacy Principles (GAPP)*, Privacy by Design (PbD), and other governance frameworks.
- In chapter 4, we introduce a privacy engineering development structure, beginning with the enterprise goals and objectives that are used to development a privacy policy.
- In chapter 5 we discuss privacy engineering requirements. We then introduce use cases and use-case metadata.
- In chapter 6, we introduce enterprise architecture and the various views of it. We dig into the privacy engineering/system engineering lifecycle methodology. We show the Unified Modeling Language (UML) usage flow from the context diagram, using the UML use-case diagram, to the use of business activity diagrams, including showing key data attributes. We move on to data an class modeling using the UML class modeling diagram, and then to user interface design. We us the system activity diagram to show where FIPPS / GAPP requirements are satisfied within the privacy component design and then we move to dynamic modeling where we define service

components and supporting metadata, including the inclusion of Privacy Enabling Technologies ~~(PETs). We then discuss the completion of development, the development of test cases, and~~ the system rollout.

- Chapter 7 discusses the Privacy Component, an app that will be used to maintain the privacy notice. The privacy team, along with the data stewards, will enter and maintain the privacy rules When an embedding program requires personal information, the privacy component will ensure that the personal information is collected according to privacy policies.
- Chapter 8 presents, as an example, a small mobile app that uses a simplified version of the privacy component to support a high school cross-country runners app.
- Chapter 9 examines a vacation planner application that utilizes a privacy component that has already been developed, tested, and implemented. A large hospitality company requires a system to help its customer community plan a vacation at one of their hospitality sites.
- Chapter 10 covers quality assurance throughout the development life cycle, data quality, and privacy impact assessments (PIA).
- Chapter 11 discusses privacy awareness assessments and operational readiness planning.
- Chapter 12 covers organizational aspects of privacy engineering, and aligning a privacy function to IT, to data governance / data stewardship, and to the security management function.
- Chapter 13 discusses how data and data privacy can be valued.
- Chapter 14 covers our musings about the future of privacy and privacy engineering, along with a privacy manifesto.

Why anyone should care about privacy, privacy engineering, or the idea o indivdual data.

It's time to serve humanity.

Humanity is people.
Humanity is empowered stewardship of our surroundings—
Our universe, planet, and future.
Humanity is described by data;
Data about humans;
Data about all things human.
Data is not humanity;
Data tells a story.
Data is not power;
Data is leverage.
Data cannot capture humanity.
Humanity can capture data.
It's time to serve humanity.
There is no one else.
We are already past due.
This is the paradox in which the privacy engineer discovers, inspires, and innovates. **Let’s begin.**

Acknowledgments

From all of us:

Our spouses and family were key members of our team, who gave us support and sacrificed much

To the wonderful team at Apress Media, particularly Steve Weiss, Jill Balzano, Nyomi Anderson and Mary Bearden, the Manifesto would likely still be in draft form were it not for your firm but encouraging hands. To Javiar Leija, Patrick Hauke, and the rest of the Intel Press team, thank you for encouraging us to convert our ideas and speeches into this book. Your guidance, experience, and generosity to a pack of newbie authors will never be forgotten. Steve, if coaching and cajoling author ever loses its charm, you have a promising career in stand-up or e-mail comedy.

To the marketing and promotions teams at Intel & McAfee, thank you for all of your support for this rather rogue project. To the wonderful Dr. Eric Bonabeau, visionary, big data, analytics, and human decision-making expert to the stars, we thank you for trusting us enough to read the manuscri and provide the Foreword that is indeed a tie to the massive data challenges that lie ahead. Your insight highlights their proximity to other, solvable, big data challenges that you and your team are tackling today. To the many contributors who selflessly heeded our calls and graciously put fingers t the keyboard and provided articles based on their real-world experiences, thank you. Your contributions not only break up the monotony of our collective voice, they also give our book deeper texture and richer content than we had ever hoped for. Our thanks to Richard Purcell and John Dutra, whose early reviews of an amorphous manuscript helped us recognize the book we were writing was manifesto, a call to action, and not just a book on engineering. Last but most certainly not least, to ou technical reviewers, Stuart Tyler and Richard Schaefer, it is impossible to thank you enough for your time, your patience, and your creativity and insights. We knew you would both be critical in shaping this book into the tool for change that we hope it will become. We were right; you were. We have loved having you all on our team.

From Michelle Finneran Dennedy:

This short section is the hardest of all to write. I am not a pithy author so I have an expansive and grateful heart. There are countless contributors, family, and friends, who remain nameless in this boo but are all known and honored by me. To the many creative and talented people who have inspired, taught, challenged, scoffed at, picked up, loved, and bought me many drinks to lament the state of privacy over the years, I thank you. To my coauthors, thank you for writing this book, keeping me on task, and putting up with my impossible dreams and making them happen. One of you taught me to walk, the other brought privacy into my life, and both have made pigs fly. To my dear husband, Tom Dennedy, your constancy and excellence as a father to our girls have kept us all going during the man months when "The Manifesto" became our sole waking activity, and I will always love you for that and for so much more. To my bright, talented, effervescent, and limitless daughters, Reilly Finn and Quincy Esther Dennedy, your future was at stake in every creative thought I have ever had in the figh for privacy. This book was written with my unfettered hope that your generation will do a better job a loving and respecting one another and the stories and information about one another that we will leav behind. You ladies are my Magnus Opus.

From Jonathan Fox:

Books, too, take a village and there are many to thank. Unfortunately, there are too many to include in one place.

There are a few, however, to whom I would like to give special recognition. First, my coauthors. Tom, I have learned much from you. Michelle, the adventure continues. Thanks to you both. Next, m wife, Nicki, you are my foundation and ballast; and my children, Sophie and Adam, your cheer and

interest in life continues to inspire.

~~Finally, there are those who helped put me on the path to this book: my parents, who introduc~~ed me to the world and encouraged me to be curious; Nancy Novogrod and Arnold Ehrlich, who introduced me to publishing; Michael Mellin, who introduced me to technology; Franz Aman, who p privacy under my watch when I was editor-in-chief of sun.com, and Kate Rundle, who had the good sense to assign a newly hired attorney named Michelle Dennedy to support the privacy program whe we were at Sun Microsystems.

To those not mentioned, your help, support, and insights are appreciated, valued, and remembere This book, like so many other things, stands on the shoulders of you and others.

From Thomas R. Finneran:

Writing and producing a book is a struggle that impacts both family and friends. Norma, my wife has supported me throughout the process, picking up the many balls that I dropped along the way. Sh facilitated the project with both actions and prayers. This has turned out to be a family project. We thank all the kids and their kids for their support.

Jonathan and Michelle had, for a number of years, been fighting the privacy wars. Michelle calle me and told me that she felt that privacy engineering was a necessity. I said that I knew how to do that. The three of us developed an outline and we were off to the races.

Contents

Part 1: Getting Your Head Around Privacy

Chapter 1: Technology Evolution, People, and Privacy

The Relationship Between Information Technology Innovation and Privacy

The Information Age

The Firewall Stage

The Net Stage

The Extranet Stage

Access Stage

The Intelligence Stage

The Dawning of the Personal Information Service Economy

Data-Centric and Person-Centric Processing

Conclusion

Chapter 2: Foundational Concepts and Frameworks

What Is Privacy?

Privacy Engineering

Personal Information

Privacy

An Operational Definition of Privacy

Fair Information Processing Principles and the OECD Guidelines

Collection Limitation Principle

Data Quality Principle

Purpose Specification Principle

Use Limitation Principle

Security Safeguards Principle

Openness Principle

Individual Participation Principle

Accountability Principle

Other Governance Standards of which to be aware

Privacy Is Not Confidentiality and Security Is Not Privacy

Confidentiality ^{1} Privacy

Security ^{1} Privacy

The Overlaps

The Disconnects

Conclusion

Chapter 3: Data and Privacy Governance Concepts

Data Management: The Management of “Stuff”

Data Governance

Benefits of Data Governance

The Privacy and Data Governance/Stewardship Connection

Data Privacy Governance Frameworks

Generally Accepted Privacy Principles (GAPP)

Impact of Frameworks on the Privacy Engineer

Frameworks Are Not the Same as Laws

Privacy by Design

How Privacy Engineering and Privacy by Design work Together

Conclusion

Part 2: The Privacy Engineering Process

Chapter 4: Developing Privacy Policies

Elements of Privacy Engineering Development

Privacy Policy Development

What Is a Good Policy?

Designing a Privacy Policy

What Should Be Included in a Privacy Policy?

General-Level Privacy Policy Development

Enterprise-Specific Privacy Development

Internal vs. External Policies

Policies, Present, and Future

Conclusion

Chapter 5: Developing Privacy Engineering Requirements

Three Example Scenarios

Example Scenario 1: The Privacy Component

Example Scenario 2: A Runner’s App

Example Scenario 3: Hospitality Vacation Planner

Privacy Requirements Engineering

Privacy Requirements Engineering

Use Cases: A Tool for Requirements Gathering

Use Cases within Privacy Engineering

Privacy Requirements Derived from Privacy Frameworks

Develop Privacy Requirement Use Cases

The Privacy Engineer’s Use of Use Case Metadata

Determining Data Requirements

How Does the Distribution Channel Impact Privacy Engineering Requirements?

Conclusion

Chapter 6: A Privacy Engineering Lifecycle Methodology

sample content of The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value

- click High Availability MySQL Cookbook
- download Behold the Black Caiman: A Chronicle of Ayoreo Life pdf, azw (kindle)
- read Our Mathematical Universe: My Quest for the Ultimate Nature of Reality book
- download online Pure Dessert: True Flavors, Inspiring Ingredients, and Simple Recipes
- click Hello, Darkness online
- Programming Grails: Best Practices for Experienced Grails Developers pdf, azw (kindle), epub, doc, mobi

- http://www.freightunlocked.co.uk/lib/Wa-and-Ga.pdf
- http://interactmg.com/ebooks/Fractures-of-the-Proximal-Humerus--Strategies-in-Fracture-Treatments-.pdf
- http://unpluggedtv.com/lib/The-Humans.pdf
- http://aneventshop.com/ebooks/The-Vietnam-War--The-History-of-America-s-Conflict-in-Southeast-Asia.pdf
- http://studystrategically.com/freebooks/Hello--Darkness.pdf
- http://serazard.com/lib/Programming-Grails--Best-Practices-for-Experienced-Grails-Developers.pdf