The Third Way to Data Privacy and Sharing – Concepts, Tools, Applications

Hypatia.Burbidge@gmail.com

Forward

This work starts with a premise, that there is a safe way to integrate computer systems while at the same time balancing civil privacy with the public government's needs and while balancing security restrictions with the sharing imperative. Accepting the premise, we can envision a future where people and systems cooperate better. Better cooperation will advance our technological-dependent civilization. A reconciliation of private and public concerns will make citizens more comfortable with a state powerful enough to pursue an aggressive national agenda.

Although the subject lies in the future, this book is not fiction. It is computer science. With the technology described here, we will build a future world better than any you can extrapolate from contemporary practices and standards. It hasn't happened yet. It hasn't been tried yet. Thus, the book runs on a line between fact and fiction, but it requires no new science, only implementation and deployment.

I plan to hand you the basic keys to the "new" computer technology. You can take the term "new" under a suspension of disbelief because the components are old and well known. We mix them together and something new emerges. We expect mixing these software components will show an unprecedented

emergent property: a high level of successful, cooperative activity conducted in a broad society of computers surpassing anything achieved to date.

That anyhow is the vision. The book provides concepts, tools and examples. Any additional talk of emergent properties and the evolution of cooperation will be relegated to a supplemental chapter in "**Error! Reference source not found.**". What you actually have here is a serious attempt to convey the computer science behind the future society of systems.

1. Setting the Scene

Setting the Scene — Why?

When interests collide, when issues polarize, when ideals are irreconcilable, society enters a time of fission —a time of division into fiercely-determined opposing camps characterized by a hostility that divides people and thwarts progress. That hostility describes the current state of the field of data privacy — people belong to one camp or another. They favor software that improves privacy or undermines it. In between the extremes there is only a wasteland devoid of proponents and suitable technology.

Tragically, our society relies more and more on privacy technology but watches helplessly as powers battle over which of two polar opposites will prevail: on one side, the privileges of the collective entities — government and corporations —to use our data for their vision of our common good or, on the other side, the rights of individual people — citizens and consumers — to own property and to decide for ourselves how our data is used.

Perhaps this description sounds too dramatic? After all, no blood is being spilled over the conflict and even the lawsuits have been relatively low key. For the most part, people takes sides only on specific issues — is Snowden a traitor or a patriot? is Google a friend or a Big Brother? does Apple obey its customers or the FBI? So far, there is little really at stake for the average citizen. Should the citizen care at all about data privacy?

This book is written because the author cares. Here is why. The battleground is quiet now but this conflict must inevitably heat up as improved technology allows the collective entities to intrude more and more on the individual's perceived rights. Also, journalists will continue to discover and publish intrusions on the public's privacy thereby embarrassing both the corporations and governments. Both will seek to preempt action and suppress opposition. You can expect more controversy and more ill-considered legislation. But, most importantly in the author's view, this battleground is a technical no-fly zone — a no man's land. Geeks usually will hack any hard problem but have left this problem entirely unattended. Anyone who is qualified is occupied building better software weapons for one side or the other (perhaps both if the pay is right). Speaking personally however, this geek abhors that vacuum and takes no pay from either side. I want to fill the vacuum and this book is part of that process.

Setting the Scene — What Subjects?

Trust, Loyalty, and Perfection

Living in a society you are connected to others. Your data protection and privacy are not yours alone; they are bound up in social interactions. Trust, loyalty and perfection are three attributes of interaction in a society. Let's examine these terms. In a society, individuals and their computer systems play assigned roles and take actions that keep the society running. Every role brings responsibilities that might be easy to bear were it not for society's complexity. Most actions require help. Every responsible individual relies on others to do part of the work, to provide part of the information, or even to accept part of the responsibility. Thus every individual is part of a complex social web. Every individual in society must trust others to help. Moreover, those who are trusted must be loyal and act as expected. Trust and loyalty are fundamental to social interaction.

Now we must mention that neither people nor their systems are prefect. Both make mistakes. As a result, trust and loyalty are not enough, society expects perfection or a close approximation.

Encryption and the Third Way

Encryption technology is a fact of life today. Knowledge of it cannot be erased. Encryption is widely available, it is simple enough that even small groups can apply it to their operations, and it is strong enough to thwart even the largest code breaking machines. We can take encryption for granted. What we can't take for granted are trust, loyalty, and perfection. All three are suspect and we can be undermined by misplaced trust, disloyal partners, and imperfect execution. This book is about how to apply encryption technology in a world where trust, loyalty and perfection are all suspect.

Given we have encryption; we have the option to encrypt all our data. But that option leaves us completely isolated with no option to shop on line, no on-line accounts with banks and no friends on the Internet. To be a part of today's world — to work, to live, and to socialize on-line —we need to share some data with others. Perfect encryption blocks that. So we compromise and let some people have some data. Once we share our data, we lose control over it. Sure you can write a nondisclosure agreement, pass legislation, or maybe sign an executive order. All that has been done. None of it can repair the damage when arbitrary limitations are simply ignored. In practice then, we are torn between a policy that locks down data leaving it unused and ineffective or sharing data and putting it at risk. Neither policy is a good one. Hence the need for a third way — an option we can select when asked to choose between locking down all data versus allowing the big players to take it at will.

The phrase "third way" commonly refers to finding a middle ground between two political agendas where the advantageous elements of both agendas are incorporated into a consensus. I'm not talking about that. What I have in mind is more the "middle way" — the Guatama Buddha's term for living in the real world being fully aware of and simultaneously striving toward two opposing goals: ascetic union with the divine versus success in this material world. The Buddhist way is not one way or the other way but a third choice. In the same way, the third way described in this book is neither private data nor collective data but a third way. It is a way forward when the other two lead to conflict and deadlock and, yes, suffering.

Setting the Scene — How?

In Part 2, we will introduce the main ideas behind the third way. Briefly, however, we can say that the third way shares specific data or allows its limited use in those cases for which the relevance of the data

can be reliably demonstrated according to a plan agreed upon in advance by the responsible parties. The third way operates inside all of the normal security protections provided by the best current practices. Current practice secures data at rest, secures it in transit, and ensures that it is used by a person or agent with a verified "right-to-know." The Third Way adds more security by insisting that the use of the data be governed additionally by a "need to know[1]." Let us compare these two policies.

A "right-to-know" policy allows or disallows the use of vast amounts of data because implementation of the policy operates on abstract, general data attributes. The policy asks whether this kind of actor has a right to use this kind of data — kind of actor and kind of data are general classifiers rather than selective specifications. A "need to know" policy is highly specific to the context and asks whether this particular actor at the present moment of time has a right to use a very specific piece of data in the context of the evidence presented with the request.

The difference between the two access policies is dramatic. When "right-to-know" policy is mistaken, it fails big. If "need-to-now" is mistaken, it fails small. In principle, what was just described could be implemented without the third way. But if one examines the real world situation in more detail, then it becomes clear that the contextual information that is provided to the decision-maker — the one who grants or denies "need to know" — is sensitive proprietary information. Thus, a decision-maker introduces another security risk which is unacceptable. In the Third Way, the decision-maker is not trusted with the information. The decision-maker is allowed to see only encrypted information. Both the protected data and the query context are encrypted during the decision regarding "need to know".

Setting the Scene — Where?

Currently, the Third Way is the road not taken. If we took it, where would it lead? In Part 3 we show three applications that exemplify the destinations along the Third Way that illustrate the concepts of solidarity, vulnerability, and new markets.

Solidarity. Things happen to people that they don't want to talk about. However, when the same thing happens to many people, they might band together and do something about the causes of their problem. That is solidarity. Fighting against solidarity is the stigma attached to victims and the afflicted. Sometimes silence seems the best way. Our example application discusses rape on campus — an event where victims feel the legal system fails. A related application would be to match patients with medical conditions to treatments or support groups, a situation where a patient might be reluctant to discuss fears and symptoms with a doctor or a group of peers.

Vulnerability to Betrayal. Many difficult situations involve a group of players who while not enemies are distrustful of each other. This situation arises naturally through competition. I want to win. So do you. Maybe we can work together but maybe I'll be better off taking advantage of you. It is a fluid situation where distrust can impede successful cooperation. Examples abound in the liaison between different intelligence services and during business negotiations.

---

[1] *Need to know is a well-known and widely applied principle of security; in the past however, it has been enforced via a subjective, manual process. What we do here is an automation of this essential function. For more see Wikipedia: https://en.wikipedia.org/wiki/Need_to_know*

New Markets. The free-enterprise market system for assets, products, and services is efficient but competitive. But competition and deregulation put some groups at a disadvantage and introduce a substantial systemic risk of market bubbles and flash crashes. Our example application builds a market where the interests of the participants are protected while maintaining competition. This example concerns a fictitious market for stock swaps. The fictitious market for stock swaps models the markets for many actual asset classes.

Setting the Scene — The Plan

This section, Part 1, makes the general case for following the Third Way. Part 2 of this book introduces concepts that are necessary to discuss the topic. Part 3 describes potential applications to illustrate how the concepts can be used to solve practical problems. The sample applications discussed in Part 3 may instruct and motivate some readers to solve additional problems in the same way. Ideally, the series of sample applications will lead by induction to a pattern for many future solutions.

Here are a few tips about how to read the book. You've already read this far. Good. If you are primarily reading to decide if the Third Way has something for you, then I'd recommend jumping forward to Part 3 — *Applications*. A look at the applications may give you some ideas. On the other hand, if you want to fully understand the Third Way then I would recommend reading all of the chapters in *Part 2 — Overview of the Concepts*.

The general question is "how to solve the data privacy problem?" In practical terms, the answer is: "write software." Because private data resides on a computer or in the cloud, any solution must be implemented with software.

Software designers and developers will be interested in the design details explained in *Part 4 — Design Considerations*. This specialized audience may also wish to evaluate and adopt implementation components discussed in *Part 5 — Tools*. While none of the active components in the public toolset is production quality, the passive ones — interfaces and protocols —could be a basis for your implementation.

The first three chapters refer to some topics without going deeply into the matter. For these topics, Chapter 6 — *Supplemental Topics* provides additional background or explanation. Lastly, detailed comments about points in the main text can be found in the *Notes* section.

About the Author(s)

The name, Hypatia Burbidge, is a nom de plume. The initial author of this work is not trying to hide. You can check him out on LinkedIn[2]. The decision not to publish under my own name is driven by the fact that the book is incomplete and unfinished in the form you see here. But it can be finished. It just takes more than one person. So my dream is that the work is carried forward by a collective of people who share the goal of a collaborative society of systems arising out of today's Internet. An architype for this collective would be the Nicholas Bourbaki group of French mathematicians.

[2] https://www.linkedin.com/in/pbaker1

If you are interested either in getting a notification when new drafts of this document are available or you would like to contribute to the work, please email to hypatia.burbidge@gmail.com.

The name chosen recognizes two great astronomers: Hypatia of Alexandria and E. Margaret Burbidge, most recently of UCSD. Astronomy is always unfinished work and we may draw some consolation that an incomplete understanding of a deep field like Astronomy can still be powerful and beautiful.

Table of Contents

Table of Contents 6

Forward 1

About the Author(s) 5

1. Setting the Scene 2

Setting the Scene — Why? 2

Setting the Scene — What Subjects? 3

Trust, Loyalty, and Perfection 3

Encryption and the Third Way 3

Setting the Scene — How? 3

Setting the Scene — Where? 4

Setting the Scene — The Plan 5

2. Overview of the Concepts ..... **Error! Bookmark not defined.**

Terminology ..... **Error! Bookmark not defined.**

Systems ..... **Error! Bookmark not defined.**

Encryption ..... **Error! Bookmark not defined.**

Roles and Functions ..... **Error! Bookmark not defined.**

Processes and Tasks ..... **Error! Bookmark not defined.**

Consent and Cooperation ..... **Error! Bookmark not defined.**

Information Fiduciaries ..... **Error! Bookmark not defined.**

Fiduciary Responsibility ..... **Error! Bookmark not defined.**

Custodian ..... **Error! Bookmark not defined.**

Curator ..... **Error! Bookmark not defined.**

Matchmaker - Exchange Markets ..... **Error! Bookmark not defined.**

Mediator ..... **Error! Bookmark not defined.**

Remote Agent Host ..... **Error! Bookmark not defined.**

Fiduciary Responsibility in a Society of Systems ..... **Error! Bookmark not defined.**

The Third Way: Use a Blind Agent Information Fiduciary ..... **Error! Bookmark not defined.**
Use Cases ..... **Error! Bookmark not defined.**
Sessions ..... **Error! Bookmark not defined.**
3. Applications ..... **Error! Bookmark not defined.**
Recognizing an Application ..... **Error! Bookmark not defined.**
Solidarity ..... **Error! Bookmark not defined.**
Campus Rape ..... **Error! Bookmark not defined.**
Private-Public Partnership: Epidemiology ..... **Error! Bookmark not defined.**
Vulnerability to Betrayal ..... **Error! Bookmark not defined.**
A Context Free Illustration ..... **Error! Bookmark not defined.**
New Marketplaces ..... **Error! Bookmark not defined.**
Example: Keeping Your Cost Factors Proprietary ..... **Error! Bookmark not defined.**
Summary of Advantages ..... **Error! Bookmark not defined.**
4. Design Considerations ..... **Error! Bookmark not defined.**
Request Tasks ..... **Error! Bookmark not defined.**
Bailout Points — Use Case 4 Reconsidered ..... **Error! Bookmark not defined.**
Checkpoints — Use Case 4 Reconsidered ..... **Error! Bookmark not defined.**
Enhanced Security — Zoned Defense ..... **Error! Bookmark not defined.**
Basic Security ..... **Error! Bookmark not defined.**
Defense Zones ..... **Error! Bookmark not defined.**
Black/White Composite Defense ..... **Error! Bookmark not defined.**
Encrypted Discovery of "Need to Know" ..... **Error! Bookmark not defined.**
Introduction ..... **Error! Bookmark not defined.**
Comparisons ..... **Error! Bookmark not defined.**
Standards ..... **Error! Bookmark not defined.**
Structured Information ..... **Error! Bookmark not defined.**
5. Tools (to be written) ..... **Error! Bookmark not defined.**
6. Supplemental Topics ..... **Error! Bookmark not defined.**
Overview of Kerckhoff's Principle, Encryption, and Keys ..... **Error! Bookmark not defined.**
Keckhoff's Principle ..... **Error! Bookmark not defined.**
Symmetric Encryption with a Single Key ..... **Error! Bookmark not defined.**
Public Key Encryption ..... **Error! Bookmark not defined.**
Other Algorithms ..... **Error! Bookmark not defined.**

Trust in Software: What You Should Know ..... **Error! Bookmark not defined.**
Software Maladies: Congenital, Acquired, and Inflicted ..... **Error! Bookmark not defined.**
Restricted Systems ..... **Error! Bookmark not defined.**
Open Source versus Proprietary Code Evaluation ..... **Error! Bookmark not defined.**
Code Signing – Single and Multiple Signatures ..... **Error! Bookmark not defined.**
White-Listing ..... **Error! Bookmark not defined.**
Similar Approaches (to be written) ..... **Error! Bookmark not defined.**
Callisto (to be written or redirected) ..... **Error! Bookmark not defined.**
IBM – Anonymous Resolution ..... **Error! Bookmark not defined.**
MIT – CryptDB ..... **Error! Bookmark not defined.**
Commentary on the Theory (to be written) ..... **Error! Bookmark not defined.**
Agency Theory (to be written) ..... **Error! Bookmark not defined.**
Evolution of Cooperation (to be written) ..... **Error! Bookmark not defined.**
Relationship with Game Theory (to be written) ..... **Error! Bookmark not defined.**
Work for the Future (to be written) ..... **Error! Bookmark not defined.**
Adjudication of Disputes (to be written) ..... **Error! Bookmark not defined.**
Index ..... **Error! Bookmark not defined.**
Table of Figures ..... **Error! Bookmark not defined.**
Notes ..... **Error! Bookmark not defined.**

Cover Photograph by Giusepe Milo *CC* [i]

[i] Photo references: Alta Badia - Trentino Alto Adige, Italy, Guisepe Milo
https://www.flickr.com/photos/giuseppemilo/