Identity Theft and Data Redaction

Stop Fighting the Last War

Richard J. Varn
Coalition for Sensible Public Records Access (CSPRA)

A Little Military History

- “Generals are notorious for their tendency to "fight the last war" -- by using the strategies and tactics of the past to achieve victory in the present. Indeed, we all do this to some extent. Life's lessons are hard won, and we like to apply them -- even when they don't apply.
- Sadly enough, fighting the last war, is often a losing proposition. Conditions change. Objectives change. Strategies change. And you must change. If you don't, you lose.”

The Maginot Line

- Probably the classic example is the French Maginot Line constructed in the aftermath of World War I. France adopted this phalanx of fortifications to prevent the Germans from repeating the August 1914 invasion that resulted in four years of bloody trench warfare.
- Unfortunately for France, Hitler and the German generals outfoxed them by inventing the blitzkrieg--a new and terrible form of lightning warfare that simply went around and over the Maginot Line.

New Weapons Defeat Old Defenses

- It is a myth however that the Maginot line ended at the Belgian border. The fortifications were connected to the Belgian fortification system, of which the strongest point was Fort Eben-Emael. The Germans broke through exactly at this fortified point with a unique assault that incorporated gliders and shaped explosive charges.

Wikipedia

Our Maginot Line

- We are trying to stop identity theft by making 30 to 60 gigabytes of data theft-proof and impenetrable
  - 300 million Americans times 100 to 200 bytes of personally identifiable information and credit card numbers
- Can anyone guarantee that can be done at all?
  - If you believe them, I have a barely used Maginot Line to sell you…
- How much has trying to do this already cost?
- What about the billions of records already on the black market?

What Is the Big Deal?

- Information is a natural resource to our modern economy and democracy
- Systems are complexly inter-related
- Government and the consumer economy is very info-dependent
- Our market economy depends on basic information equity
- Neither the benefits nor the costs of information restriction are apparent or even known—proceed with caution

Why Do We Keep Fighting the Last War?

- How can I say this nicely?
  - They do not get it
  - They are not even trying very hard
- The reporting and public education is lagging
- The analysis is meager, the resources few
- The crooks are too well financed and highly motivated
- Because government has the most control over its own records, it tries to solve the problem there

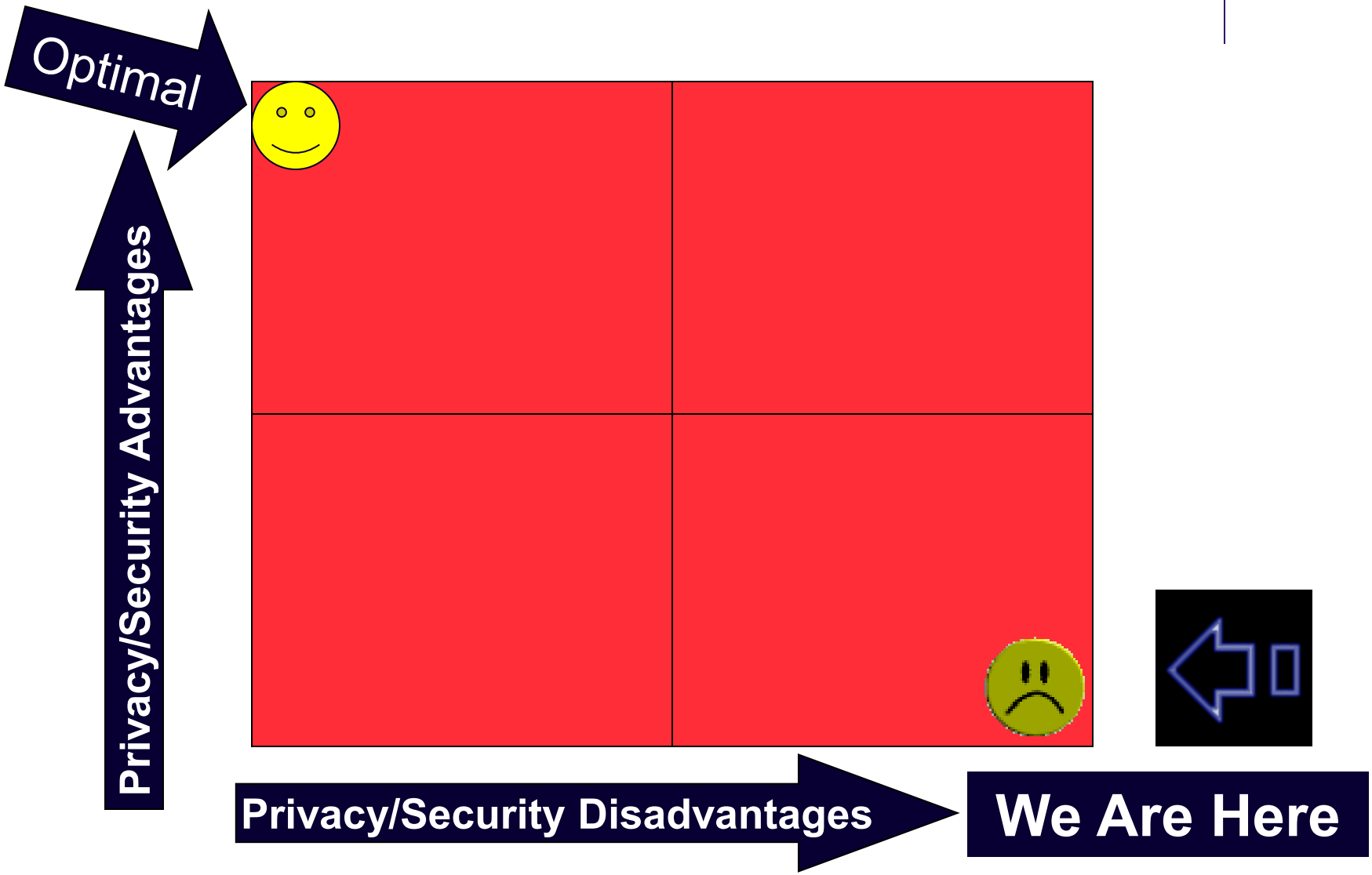
Public Records Are Not The Problem

- Un-validated, single factor authentication and a highly-evolved and unchecked cybercrime industry are the primary causes of identity theft, fraud, malware, phishing, cyber attacks, and crime, not personal data available in public records
- It is as if just knowing your street address gave anyone the key to enter your house
- Weak, single factor authentication allows fraudulent access to many rights, benefits, and privileges
- Information alone is used to allow transactions

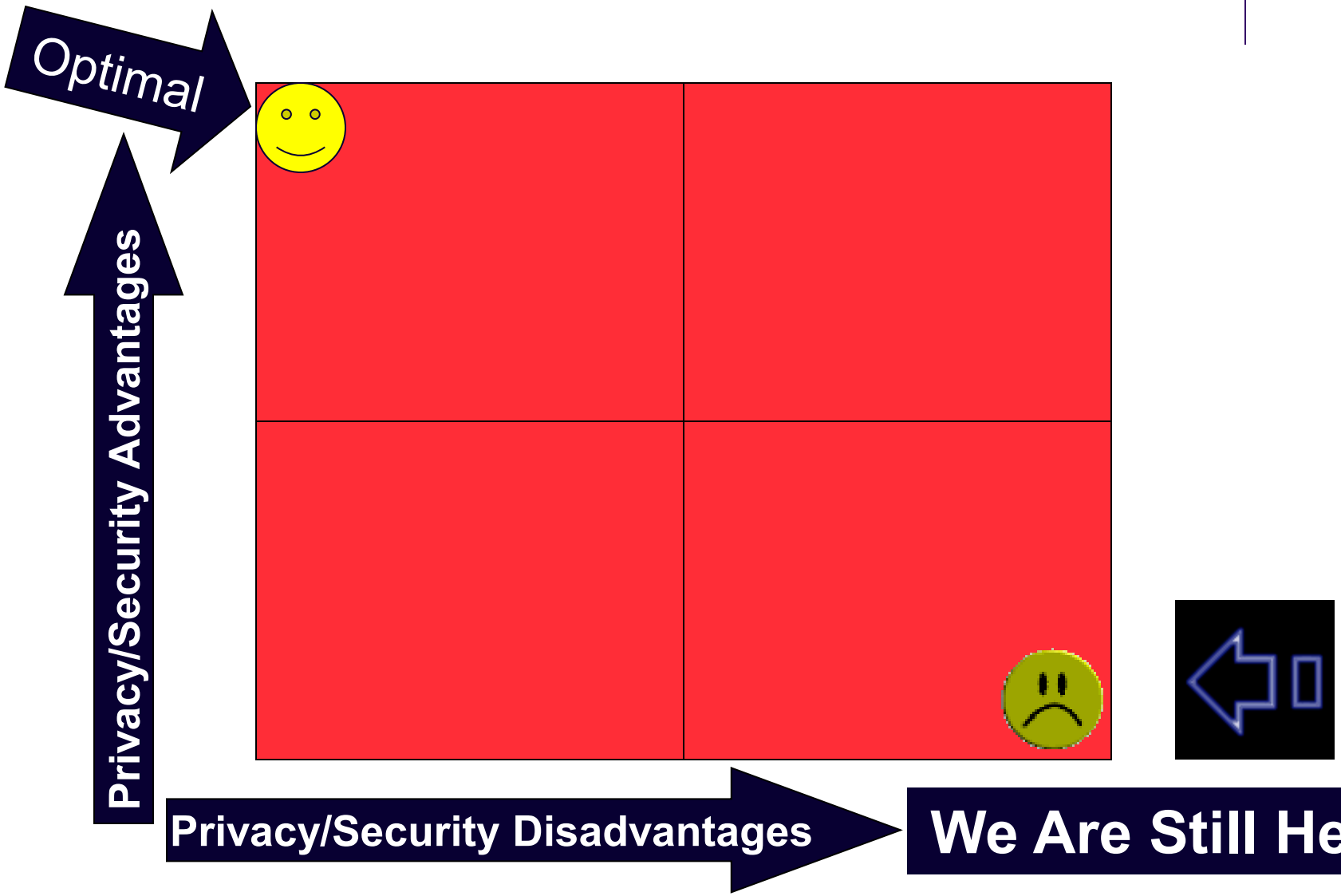
Everyone But Us

- All of the world's functioning democracies have a nation identity management system and/or a national ID card (NIDC)
- Having such systems have not been causally connected to a rise in authoritarianism
- We are not likely to get a NIDC anytime soon
- We have several systems like Real ID, but they are not used in a way that would address the many problems of risk management and identity theft and fraud

No National Identity Card



Having a National Identity Card



But the Horse Is Gone…

- So, we need to attack the cybercrime industry and the way they monetize data theft and malware, not the information industry and open government
- Numerous jurisdictions are attacking the problem in the wrong way
- By redacting public records and limiting access, we are in danger of fighting the last war against cyber criminals who already have the data and tools they need to commit crimes

Nail It Shut Anyway…

- The private sector has addressed the lack of a common national identity management system with many services on which residents, businesses, governments, and our economy depend
- There are massive administrative, cost, and feasibility issues with hiding a few letters and numbers and massive unintended costs and consequences inevitably follow
- Hiding those letters and numbers from the private sector destroys the private identity management systems on which we routinely depend

We Are the Good Guys

- We are not distinguishing or appreciating the legitimate uses
- Many commercial public records users already have complete identity information
- A combination of a few identifiers help match up with information they already have (often from the subject of the record) and satisfy legal requirements
- Why hesitate to give it to them again from the public record?
- Press should also have access for public accountability and transparency

Who Are You?

- Names are not unique while numbers, paired with a name, can be unique
- Without the ability to uniquely identify the subject of a record, the very people we want to protect will be those most harmed by false positive and false negative findings derived from incomplete and inaccurate public records
- Try it yourself: how would you verify a person's identity or tell two people apart with only names?

Vocabulary

- Identity—the one and only you
- Biometrics
- Enrollment
  - You are what databases and documents say you are

Who and What

- Authentication
  - Three pillars of proper authentication
    - Know
    - Own
    - Are
- Authorization

Authentication

- Using the proper number, kind, and mix of factors to authorize a person or attribute behaviors is the critical step we are missing
- Our choice of factors must be tied to the risk inherent in the transaction or attribution
- “Red Flag” rules are one model

Distinctions

- **Privacy and Access**—the who, what, when, where, why, and how policies on data and records
- **Security**—the enforcement of privacy policies
- **Integrity**—maintenance and protection of records from accidental or purposeful alteration or loss
- **Accuracy**—quality assurance and a process to detect and correct errors

Enforce v Surveil

- Enforcement
  - Administrative
  - Civil
  - Criminal
  - Private
- Surveillance
  - Public
  - Private
  - Government

How We Get These

- Permissions
- Privileges
- Rights
- Benefits

- Anonymously
- Pseudonymously
- Verinonymously
  - With proof of identity adequate for the risk and value of the activity or transaction

Data Management

- Mining
- Matching
- Use
  - Unlimited, limited governmental or private use, transactional use only, third party use only, infomediary use, gatekeeper use, and for public purpose use where the government is not the custodian

Key Questions of Data Management

- Who can see?
- Who has seen?
- Who can change?
- Who has changed?
- Who can use and for what?
- Who has used and for what?

How Do I Know You?

- Personally identifiable information
- De-identified personal information
- Anonymous information
- Non-personal information
- Virtual obscurity

We Require Accuracy in Identity and Data

- Protecting vulnerable populations
- Enforcing laws
- Complying with laws
- Risk management
- Lending and credit
- Fairness
- Fact checking and correlation of facts for reporting

Laws, Rules, Rights, and Processes Requiring ID/Data Management

- State public records laws
- Court records
- Law enforcement
  - Entrance and exit from the system
- FCRA
- Hiring, immigration, and background checks
- HIPAA
- Real ID Act
- DPPA
- Age restricted products
- State privacy laws
- Personnel records
- Taxpayer privacy
- Employment discrimination
- Sexual harassment
- Workplace rules
- Management of and access to data facilities and personal data
- Administration of laws
- Transportation laws
- GLBA/FINRA/Red Flag Rules

Public Records are Critical to Compliance

- Court records, financial filings, criminal history, and professional licenses
- Birth and immigration documents
- Death
- Name change
  - Marriage
  - Aliases and businesses
- Driver's License

No, Just Say, “Charge It!”

- According to Liz Pulliam*: “Merchants' agreements with Visa, MasterCard, American Express and Discover specifically forbid the retailers from requiring identification. Your signature is supposed to be enough. The store clerk shouldn't even *ask* for ID per Visa and MasterCard rules. American Express and Discover don't prohibit asking but strongly discourage it.”
- WHY?!? (hint: it starts with a $)

* http://articles.moneycentral.msn.com/Banking/FinancialPrivacy/can-stores-really-ask-you-for-that.aspx?page=2

Consequences

- How many identities should a person have?
- Should a person be able to avoid the consequences of their actions by pretending to be someone else or by having duplicate or incomplete records?
- How can we enforce our laws and society's rules without access to true information and identity security?

Cybercriminals Adopt and Adapt

- Phishing, Malware, Botnets, and Cybercrime As A Service
- They are faster at adopting tools of attack than we are at adapting our defenses and going on the offensive
- We desperately need more cybercops and intergovernmental cooperation

Machines Directed by Crooks

- Criminal money is backing the same kind of investments, technology, and services that the legitimate economy backs, and it works
- Millions compromised machines
- AI enabled hacking
- Cryptocurrencies now support the financing and payout

Identity(?) Theft

- Javelin Study (not done anymore)
- Vast majority is direct hacking, card fraud, and account theft, not using PII to create new accounts
- Stolen credentials and cybercrime services are very cheap or very cost effective
- Billions of credentials and identities available on the black market

Why Do You Rob Banks, Willie?

- Steal account access, not identity
- Cyber protection rackets and blackmail
- Hack and attack the source of the money and goods and just steal it from them directly
- Wholesale crime, not retail

Key Findings and Countermeasures

- Stolen cards and card numbers are the largest sources of loss
- Stolen authentication credentials and passwords and compromised machines are the keys to theft
- Notice and vigilance cut losses to a minimum
- ID theft monitoring, prevention, and insurance services are the best way for an individual to protect themselves

Count the Moving Parts

- Stop data loss from every user, computer, device, server, network, IT worker, person with access, application, database, datacenter, and storage medium
- That's just a few trillion failure points

ORRRRRR…

- Fix our identity security system and its use in transactions

Fighting Back

- “…we shall fight on the beaches, we shall fight on the landing grounds, we shall fight in the fields and in the streets, we shall fight in the hills; we shall never surrender…until, in God's good time, the New World, with all its power and might, steps forth to the rescue and the liberation of the Old .”

Winston Churchill

Get Out of the Foxhole

- ”You'll never get the Purple Heart hiding in a foxhole! Follow me!"
  Captain Henry P. Jim Crowe - 13th January 1943 - (Guadalcanal)
- Hit the cybercrooks where they live
- Move from Digital Loss Prevention to better strategies
- Monitor, prevent, and insure against the cost of misuse

Get Out of the Foxhole

- Create a US Identity Security System
- Create “transaction management as a service”
  - No to all
  - If X, then yes
  - Ask before X
  - Escalate proof requirements if X
  - Yes, to all as I really don’t have anything to steal
- Use Digital Data Use Prevention
- Start Digital Data Theft Detection

Questions?

Richard J. Varn
Coalition for Sensible
Public Records Access
http://www.cspra.org