

# Categorizing, Analyzing, & Managing Third Party Trust

Andy Sayler

TPRC44

10/01/16



University of Colorado **Boulder**

# The Internet



# Third Party Services

# Questions

What capabilities are we entrusting  
to third parties?

What capabilities are we entrusting  
to third parties?

**How can this trust be violated?**

What capabilities are we entrusting  
to third parties?

How can this trust be violated?

**Can we reduce the degree  
of required trust?**



What capabilities are we entrusting  
to third parties?

How can this trust be violated?

Can we reduce the degree  
of required trust?

Can we reduce the likelihood  
of trust violations?

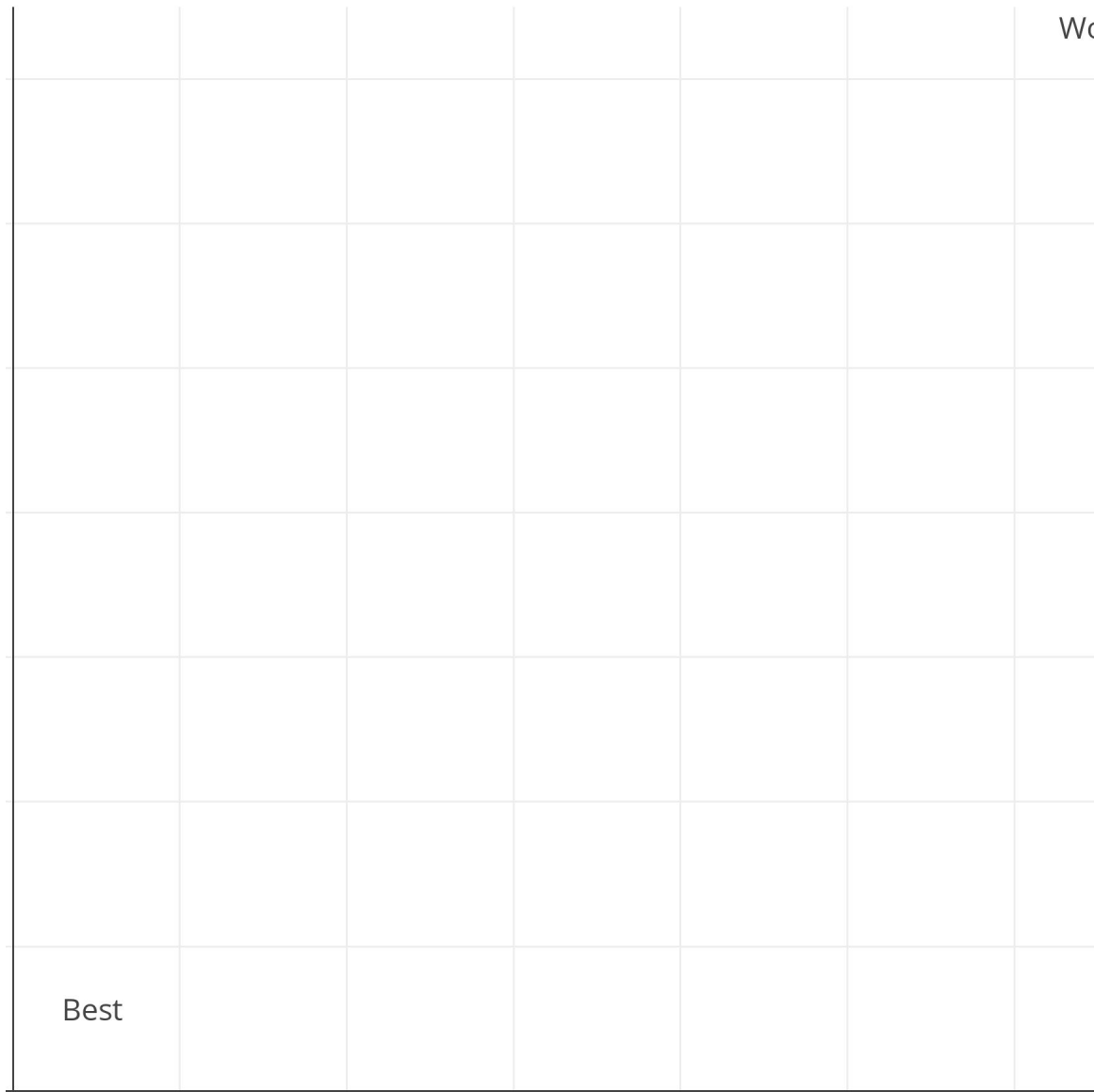
# Modeling Trust

# Degree of Trust (Capabilities)

Degree of Trust  
(Capabilities)

Types of Violation  
(Attacks)

Risk of Violation



Worst

Best

Degree of Trust



# Degree of Trust

Storage (S)

Access (R)

Manipulation (W)

Meta-Analysis (M)

# Types of Violation

Implicit (P)

Compelled (C)

Unintentional (U)

Colluding (L)

# Degree of Trust

Storage (S)

Access (R)

Manipulation (W)

Meta-Analysis (M)

# Types of Violation

Implicit (P)

Compelled (C)

Unintentional (U)

Colluding (L)

# Degree of Trust

Storage (S)

Access (R)

Manipulation (W)

Meta-Analysis (M)



# Degree of Trust

## Storage (S)

*Can a third party faithfully store private user data and make it available to the user upon request?*

Access (R)

Manipulation (W)

Meta-Analysis (M)

# Degree of Trust

Storage (S)

Access (R)

*Can a third party read and interpret  
the private user data they store?*

Manipulation (W)

Meta-Analysis (M)

# Degree of Trust

Storage (S)

Access (R)

Manipulation (W)

*Can a third party modify the  
private user data to which they have access?*

Meta-Analysis (M)

# Degree of Trust

Storage (S)

Access (R)

Manipulation (W)

**Meta-Analysis (M)**

*Can a third party gather user metadata  
related to any stored private user data?*

# Examples





Storage (S)



Storage (S)  
Access (R)





Storage (S)  
Access (R)  
Manipulation (W)



Storage (S)  
Access (R)  
Manipulation (W)  
Meta-Analysis (M)



Storage (S)

Access (R)

Manipulation (W)

Meta-Analysis (M)



Storage (S)

Access (R)

Manipulation (W)

Meta-Analysis (M)

# Degree of Trust

Storage (S)

Access (R)

Manipulation (W)

Meta-Analysis (M)

# Types of Violation

Implicit (P)

Compelled (C)

Unintentional (U)

Colluding (L)

# Degree of Trust

Storage (S)

Access (R)

Manipulation (W)

Meta-Analysis (M)

# Types of Violation

Implicit (P)

Compelled (C)

Unintentional (U)

Colluding (L)

# Types of Violation

Implicit (P)

Compelled (C)

Unintentional (U)

Colluding (L)

# Types of Violation

## Implicit (P)

*Occurs when a third party violates a user's trust in a manner approved by the third party.*

Compelled (C)

Unintentional (U)

Colluding (L)



# Types of Violation

Implicit (P)

Compelled (C)

*Occurs when a third party is compelled by another actor to violate a user's trust.*

Unintentional (U)

Colluding (L)

# Types of Violation

Implicit (P)

Compelled (C)

Unintentional (U)

*Occurs when a third party  
unintentionally violates a user's trust.*

Colluding (L)

# Types of Violation

Implicit (P)

Compelled (C)

Unintentional (U)

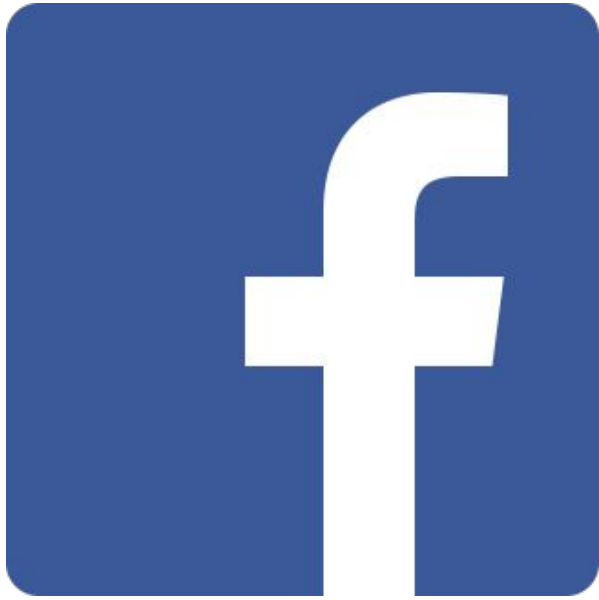
**Colluding (L)**

*Occurs when multiple trusted parties collude to gain capabilities beyond what the user intended each to have.*

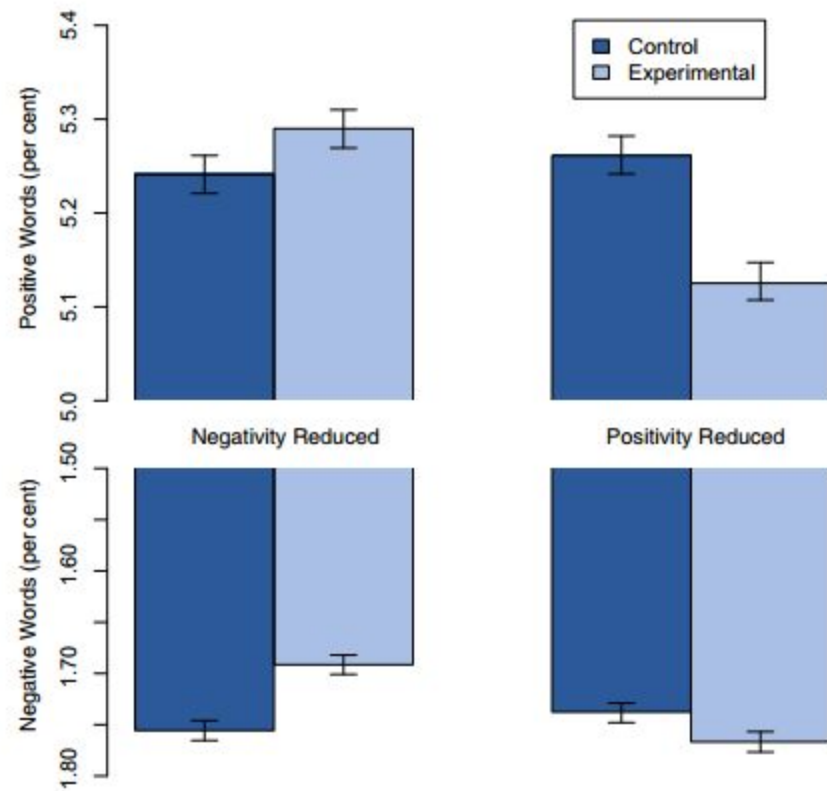
# Examples

# Implicit Violations

# Implicit Violations



# Implicit Violations



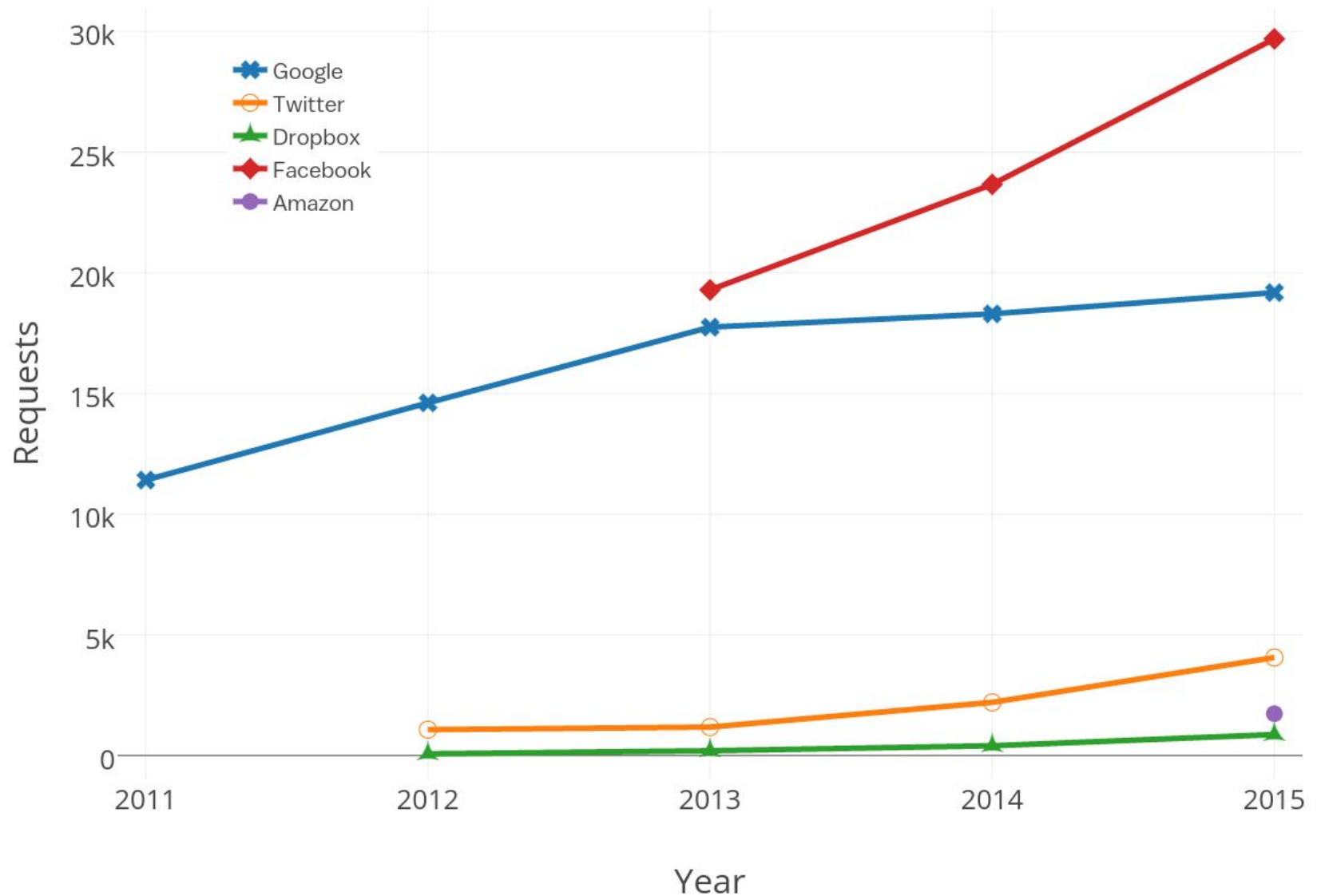
**Fig. 1.** Mean number of positive (*Upper*) and negative (*Lower*) emotion words (percent) generated people, by condition. Bars represent standard errors.

# Compelled Violations



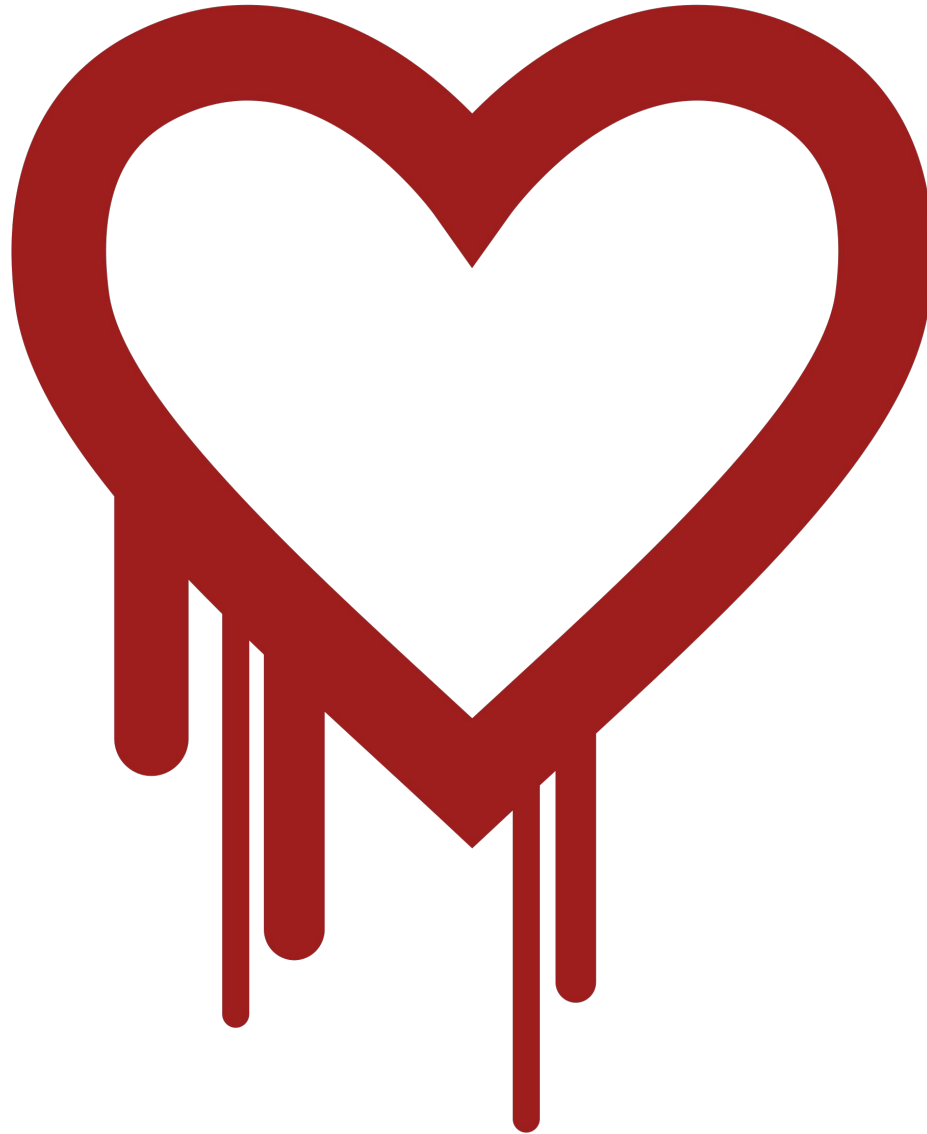
# Compelled Violations

Number of Successful USG Data Requests by Year



# Unintentional Violations

# Unintentional Violations



# Collusion Violations

# Collusion Violations



# Managing Trust

# Degree of Trust

Storage (S)

Access (R)

Manipulation (W)

Meta-Analysis (M)

# Types of Violation

Implicit (P)

Compelled (C)

Unintentional (U)

Colluding (L)

# Degree of Trust

Storage (S)

Access (R)

Manipulation (W)

Meta-Analysis (M)

# Types of Violation

Implicit (P)

Compelled (C)

Unintentional (U)

Colluding (L)





Storage (S)

Access (R)

Manipulation (W)

Meta-Analysis (M)



Storage (S)

Access (R)

Manipulation (W)

Meta-Analysis (M)



Storage (S)

Access (R)

Manipulation (W)

Meta-Analysis (M)

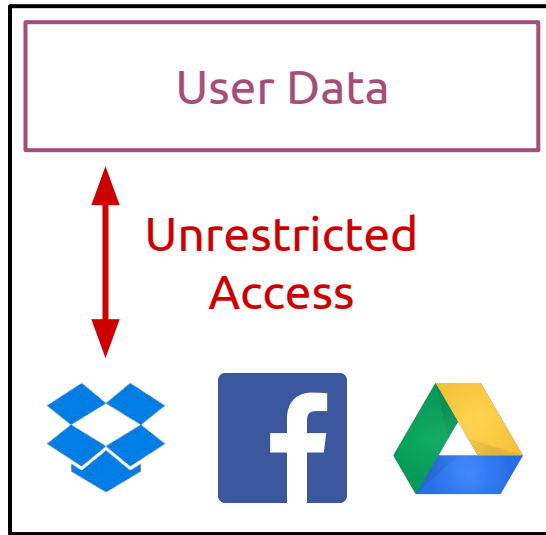
# Trust Surplus

Access (R)

Manipulation (W)

# Traditional Trust Model

Feature Provider

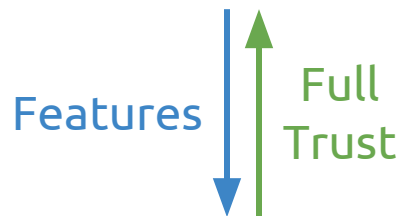


Storage (S)

Access (R)

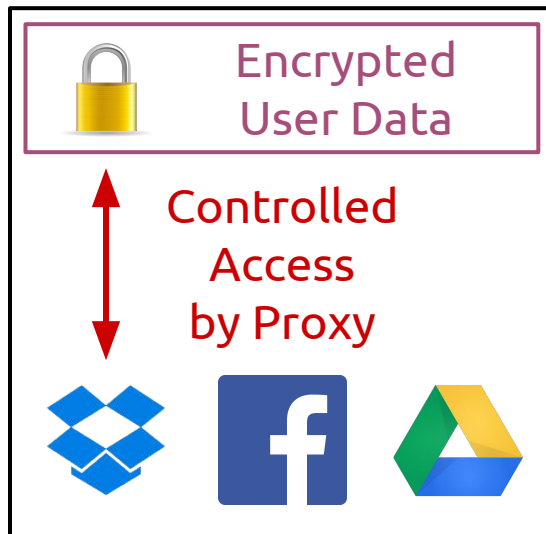
Manipulation (W)

Meta-Analysis (M)



# Client Trust Model

Feature Provider

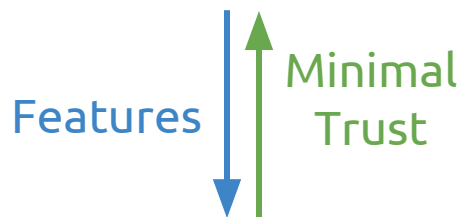


Storage (S)

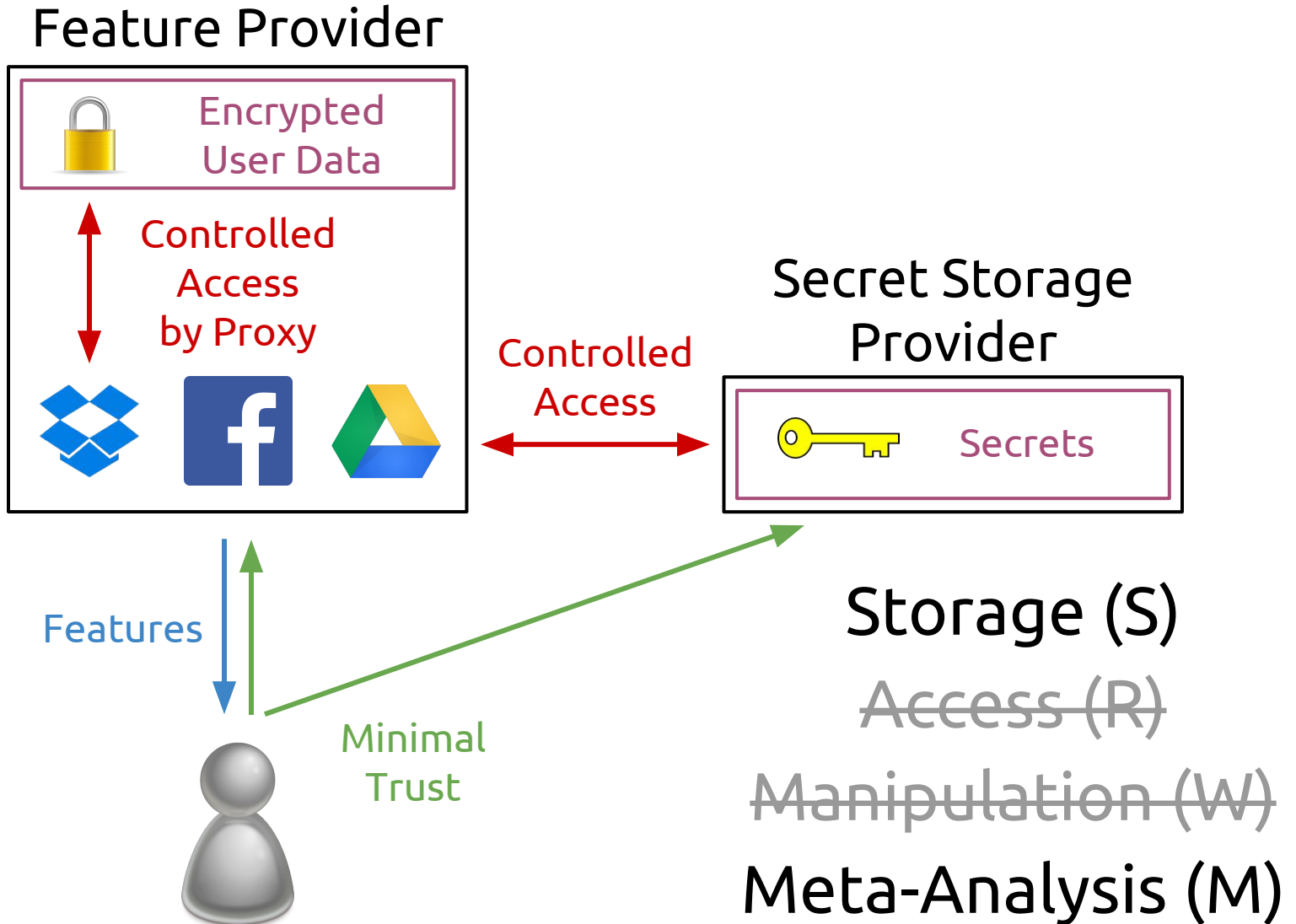
~~Access (R)~~

~~Manipulation (W)~~

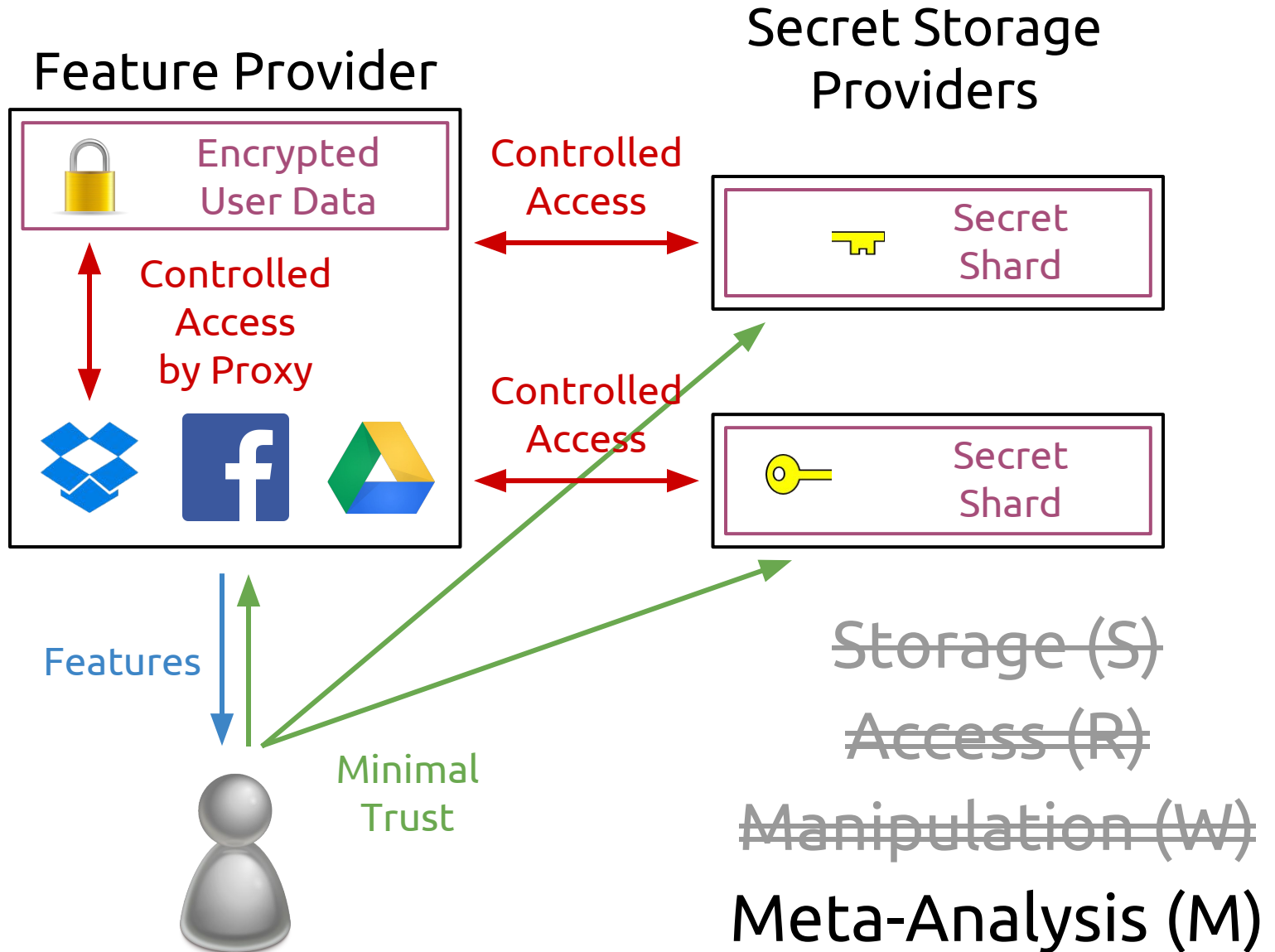
Meta-Analysis (M)



# Distributed Trust Model



# Distributed Trust Model





# Distributed Trust Model

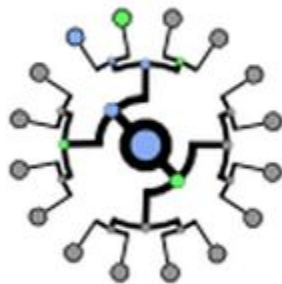


# Distributed Trust Model



MILAGRO

# Distributed Trust Model



Certificate  
Transparency

# Degree of Trust

Storage (S)

Access (R)

Manipulation (W)

Meta-Analysis (M)

# Types of Violation

Implicit (P)

Compelled (C)

Unintentional (U)

Colluding (L)

# Degree of Trust

Storage (S)

Access (R)

Manipulation (W)

Meta-Analysis (M)

# Types of Violation

Implicit (P)

Compelled (C)

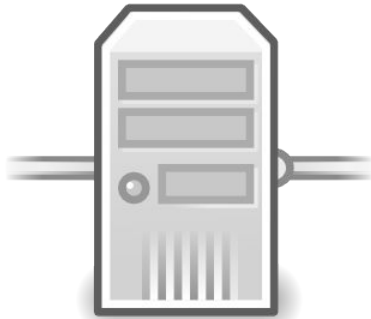
Unintentional (U)

Colluding (L)

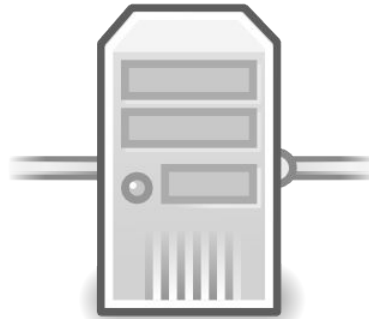
# Distributed Trust Markets

# Distributed Trust Markets

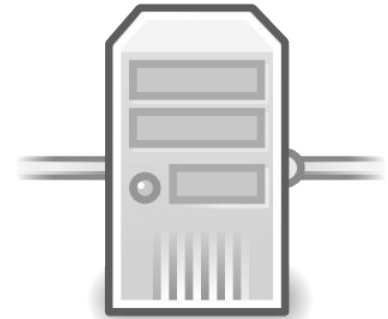
Storage Provider



Storage Provider



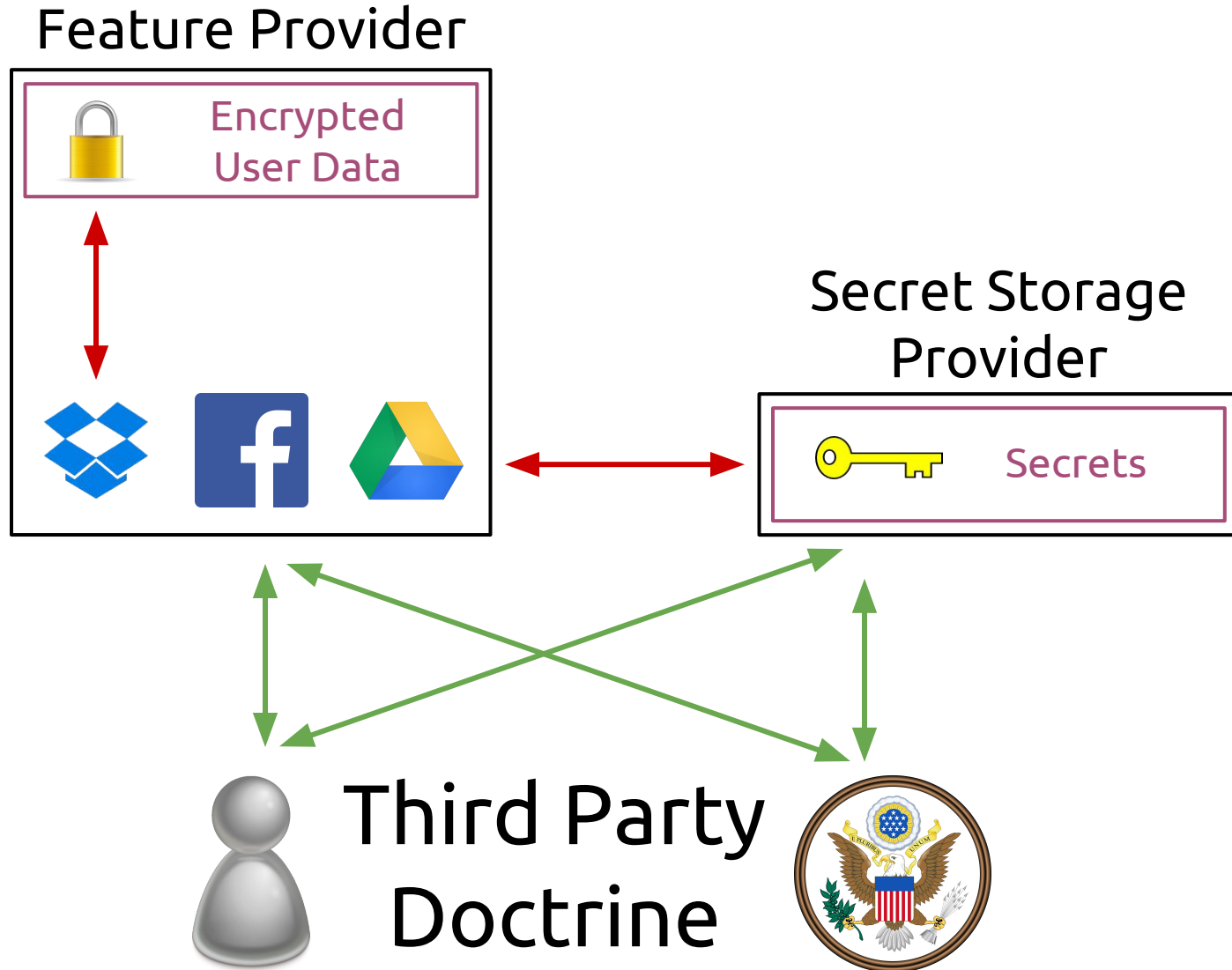
Storage Provider



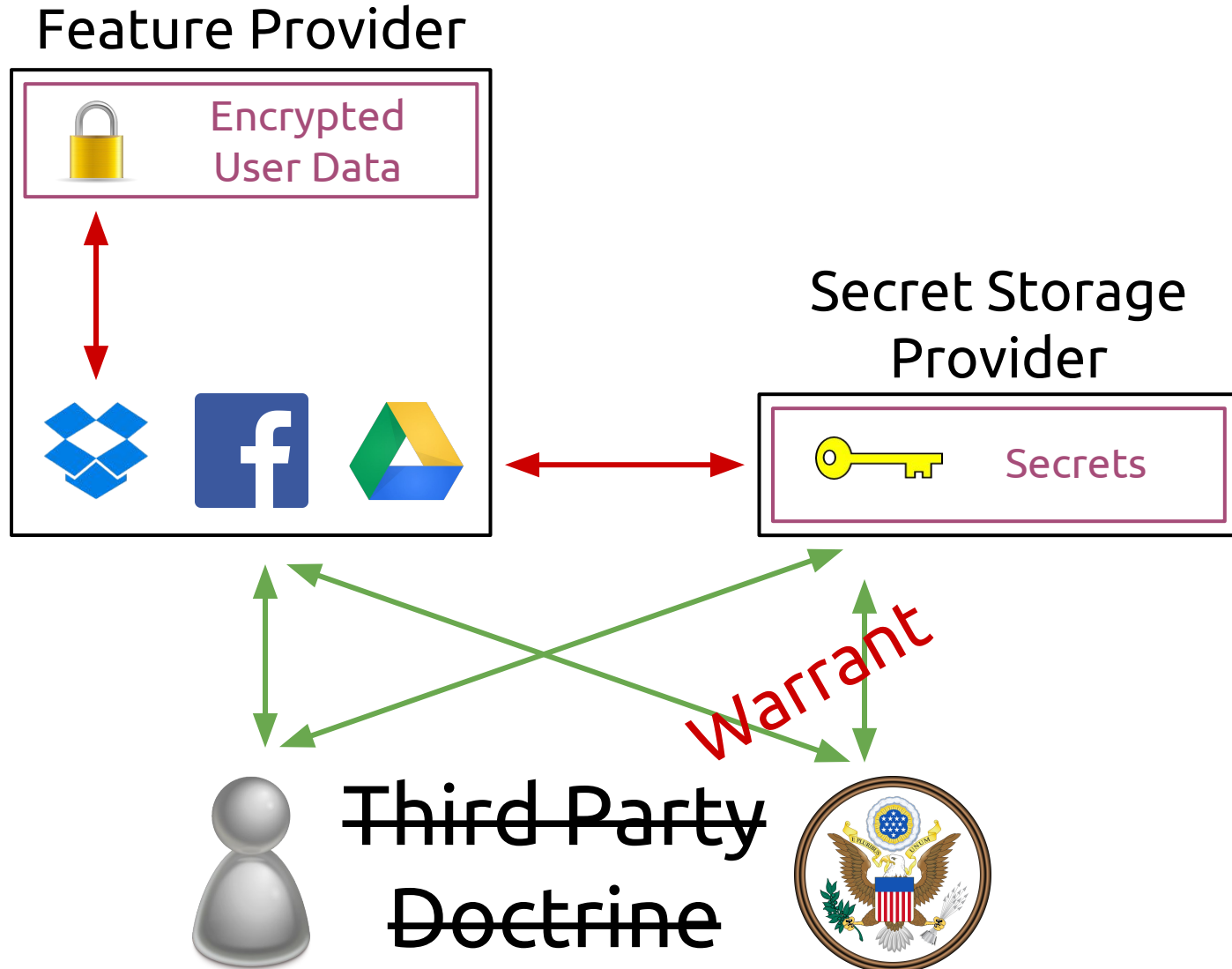
# Digital Due Process



# Digital Due Process

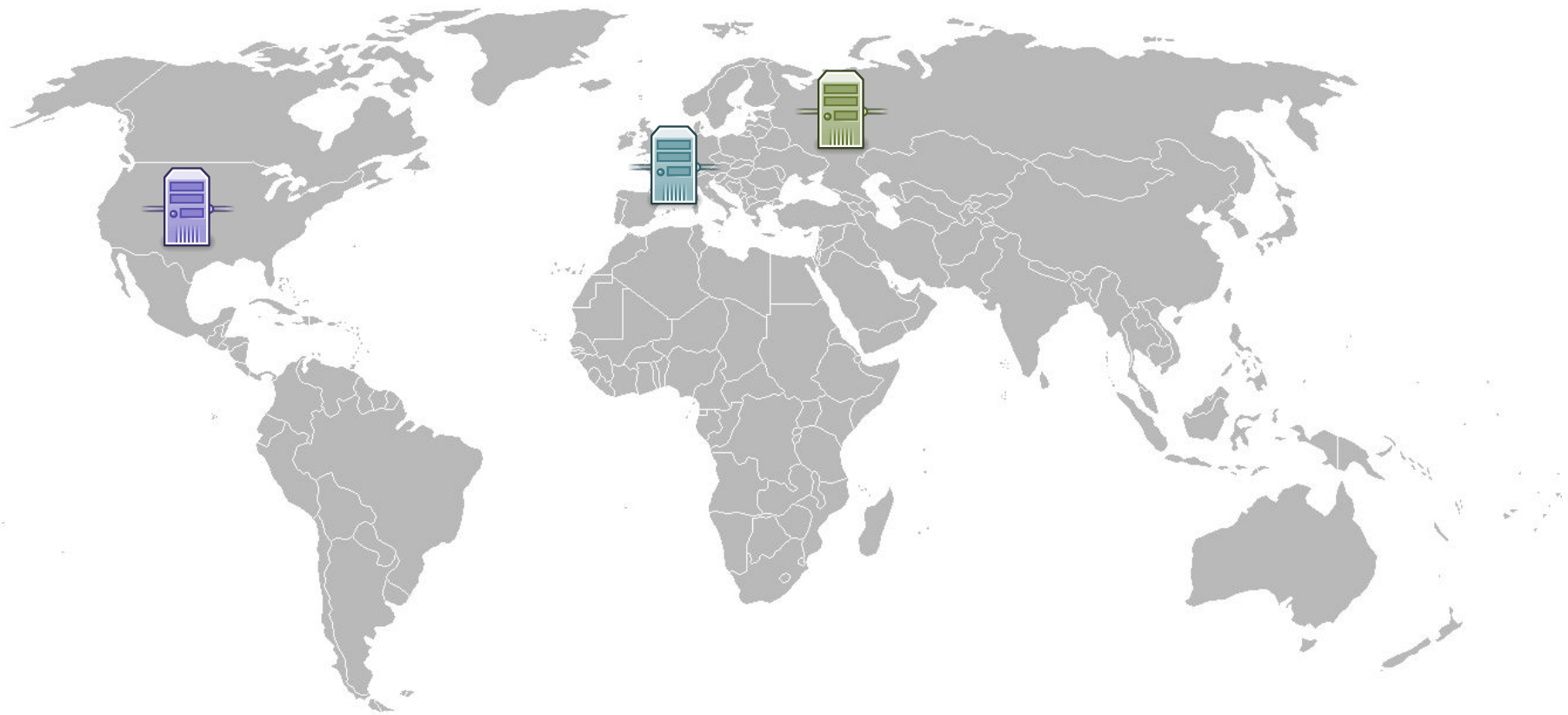


# Digital Due Process



Alternatively...

# Alternatively...



## Jurisdictional Arbitrage

# Third Party Liability

# Third Party Liability

Storage Provider



Liability

# Third Party Liability

Storage Provider



Liability



Insurance

# Third Party Liability

\$\$\$ ?



Secrets

Liability

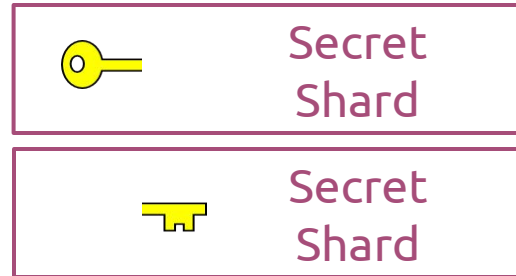


Insurance



# Third Party Liability

\$\$\$ ???



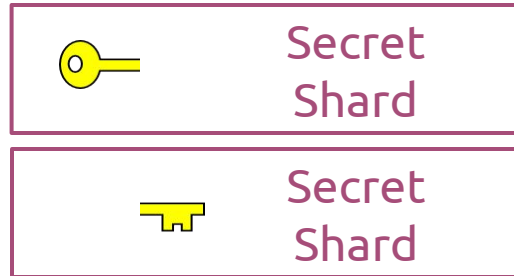
Liability



Insurance

# Third Party Liability

Declare \$\$\$



Liability



Insurance

# Conclusion

What capabilities are we entrusting  
to third parties?

How can this trust be violated?

Can we reduce the degree  
of required trust?

Can we reduce the likelihood  
of trust violations?

Thank You

Questions?

Extra Slides

# LastPass...

Storage (S)

~~Access (R)~~

Manipulation (W)

Meta-Analysis (M)





tresorit

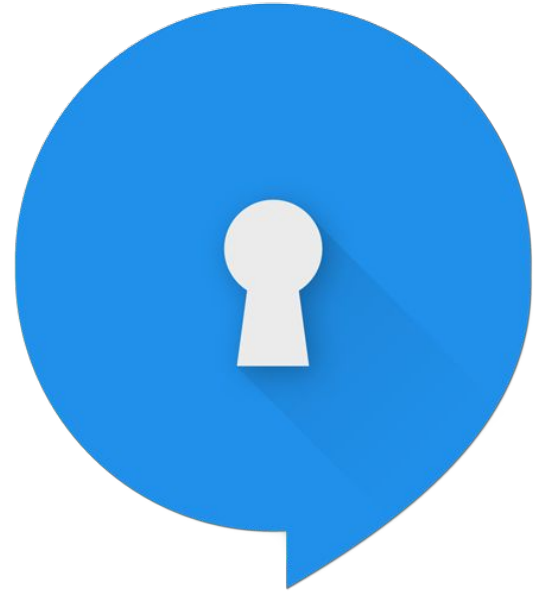


Storage (S)

~~Access (R)~~

~~Manipulation (W)~~

Meta-Analysis (M)



Storage (S)

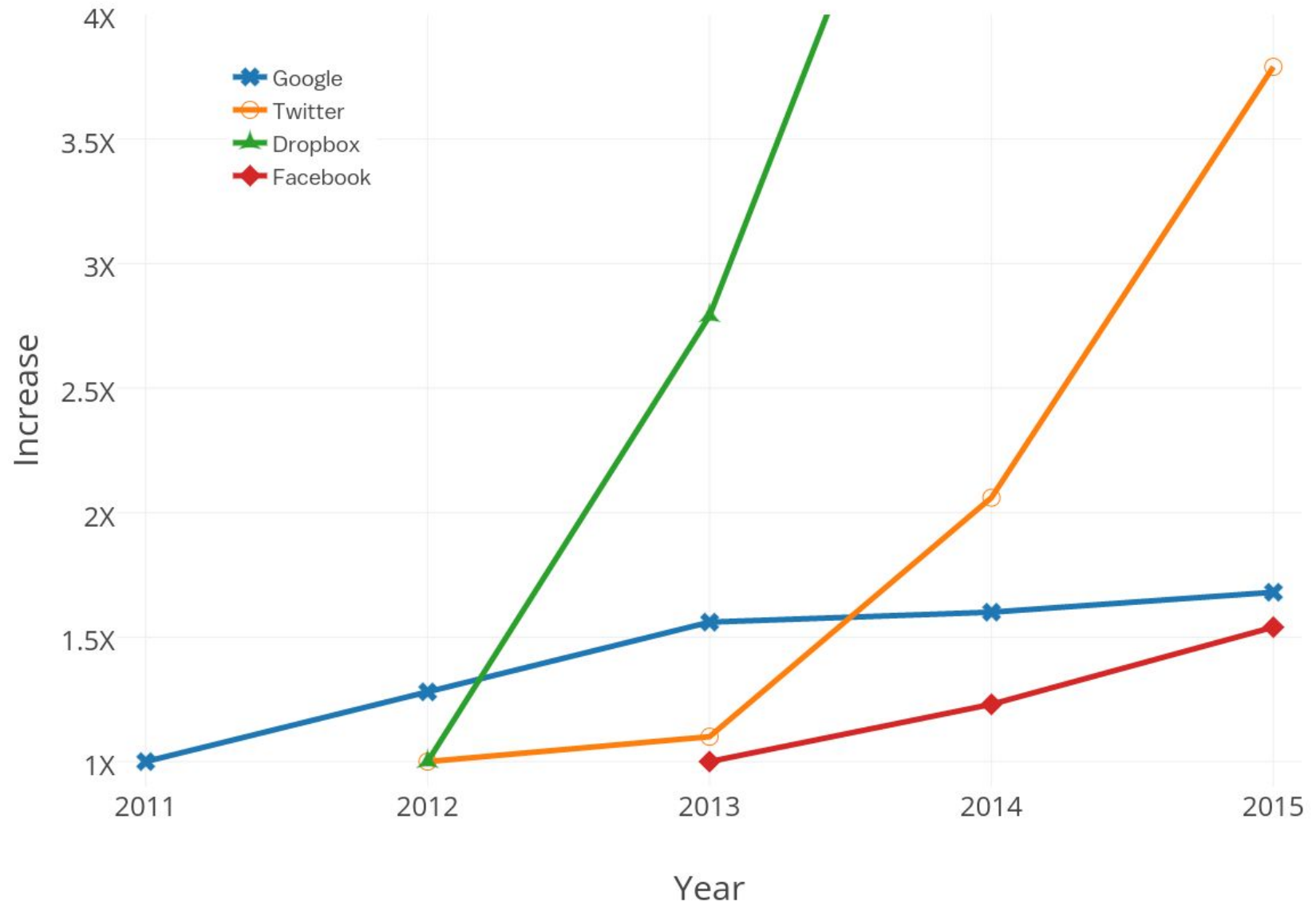
~~Access (R)~~

~~Manipulation (W)~~


~~Meta-Analysis (M)~~

# Compelled Violations

Increase of Successful USG Data Requests by Year



# Compelled Violations



[Email Updates](#)[Court Locator](#)[Careers](#)[News](#)[Listen to This](#)

[Home](#)[About Federal Courts](#)[Judges & Judgeships](#)[Services & Forms](#)[Court Records](#)

## Services & Forms

[Bankruptcy](#)

[★ Bankruptcy Basics](#)

[Filing Without an Attorney](#)

[Credit Counseling and Debtor Education](#)

[Trustees and Administrators](#)

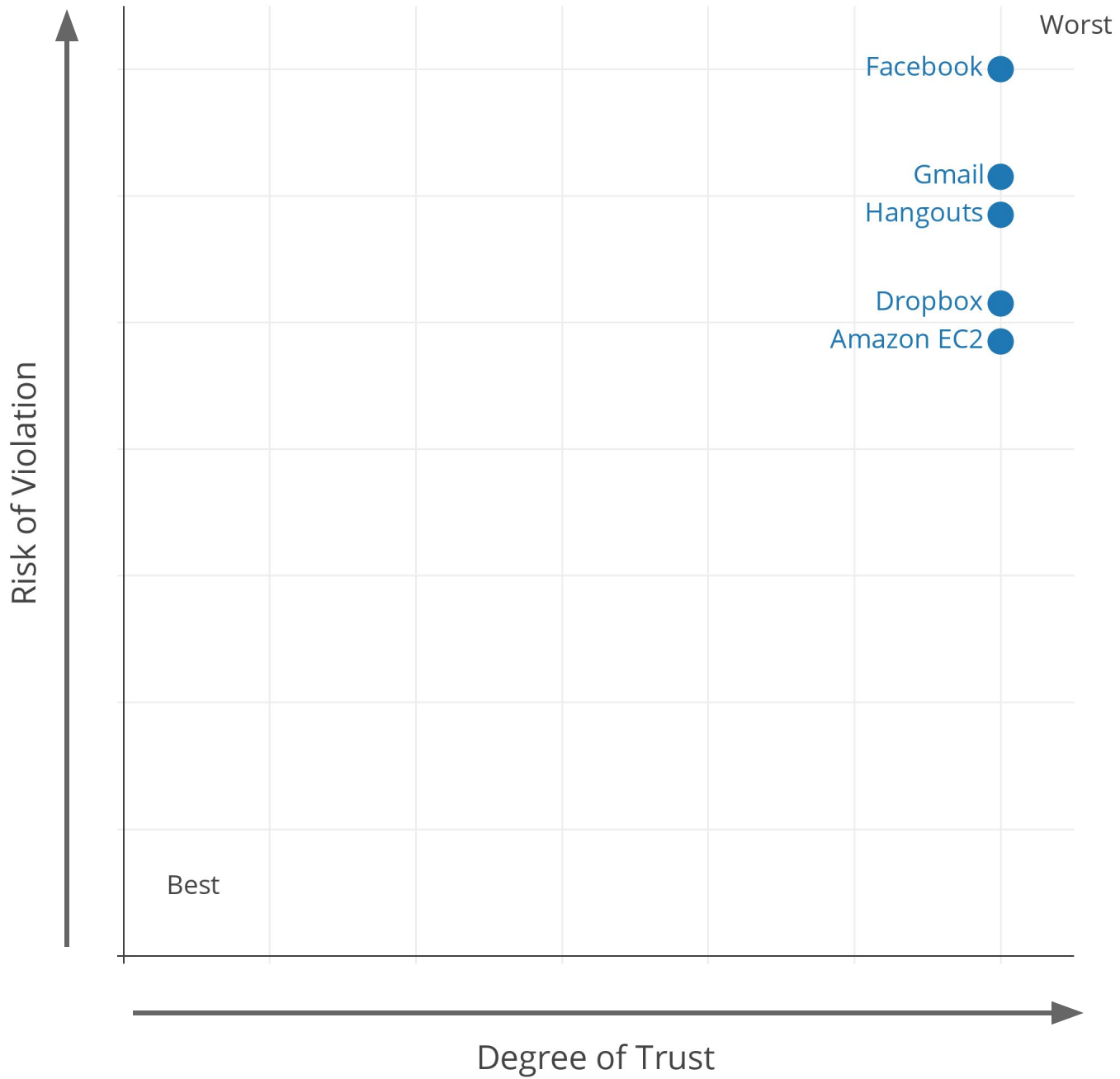
[Approved Bankruptcy Notice Providers](#)

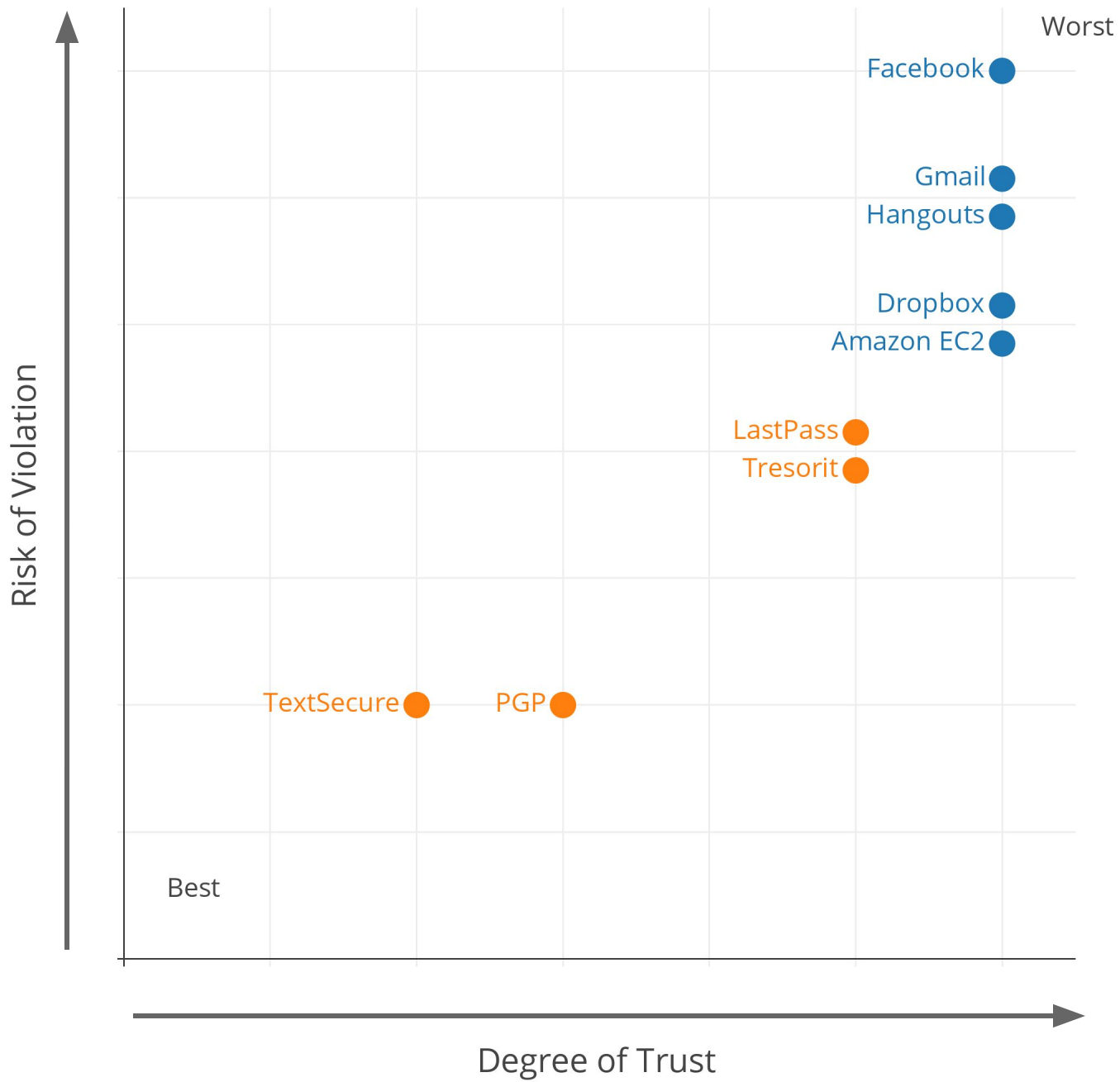
## Chapter 11 - Bankruptcy Basics

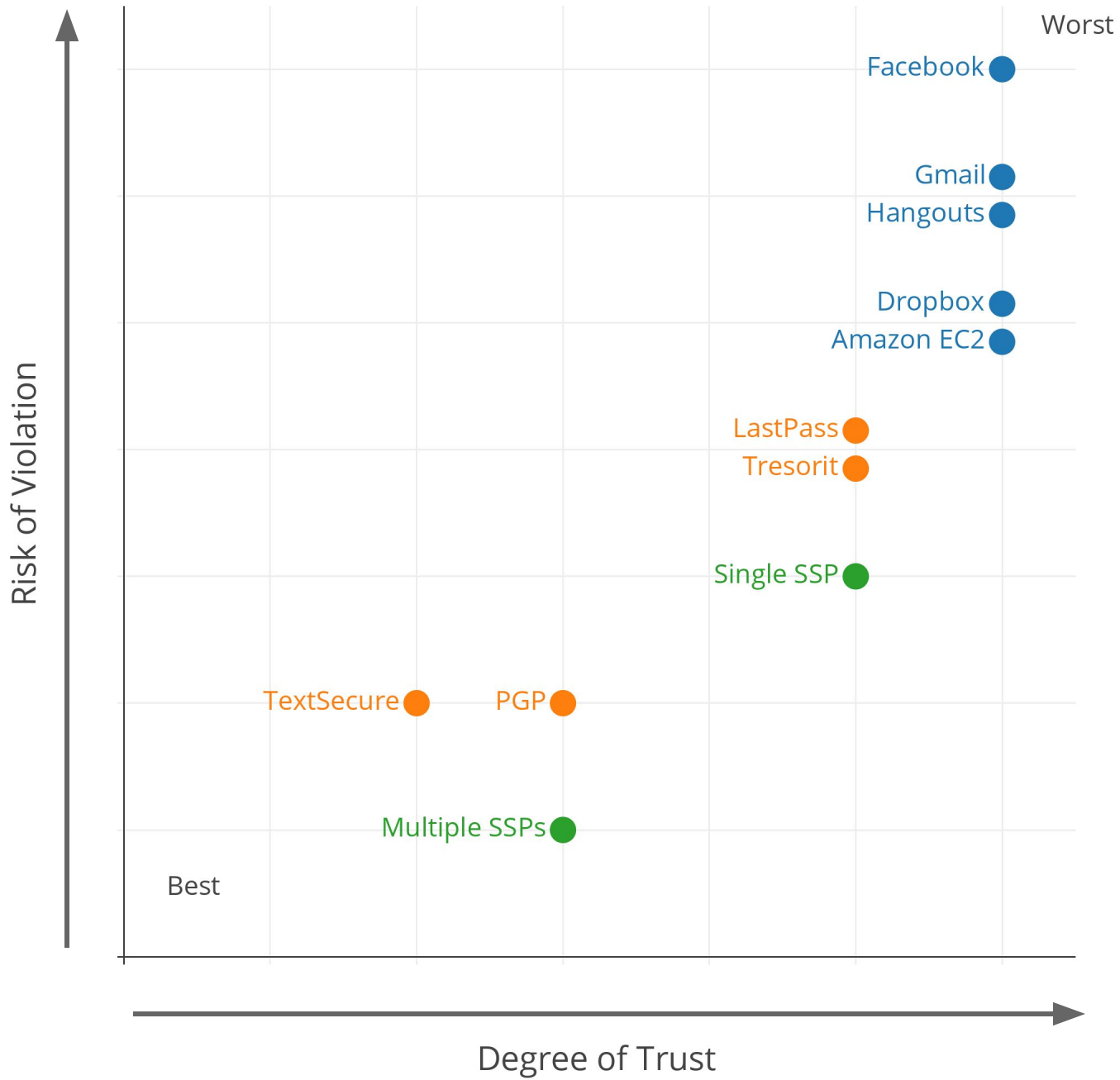
*This chapter of the Bankruptcy Code generally provides for reorganization, usually involving a corporation or partnership. A chapter 11 debtor usually proposes a plan of reorganization to keep its business alive and pay creditors over time. People in business or individuals can also seek relief in chapter 11.*

### Background

A case filed under chapter 11 of the United States Bankruptcy Code is frequently referred to as a "reorganization" bankruptcy.







Application	Storage	Access	Manipulation	Meta-analysis	Score

Degree of Third Party Trust Across Capabilities





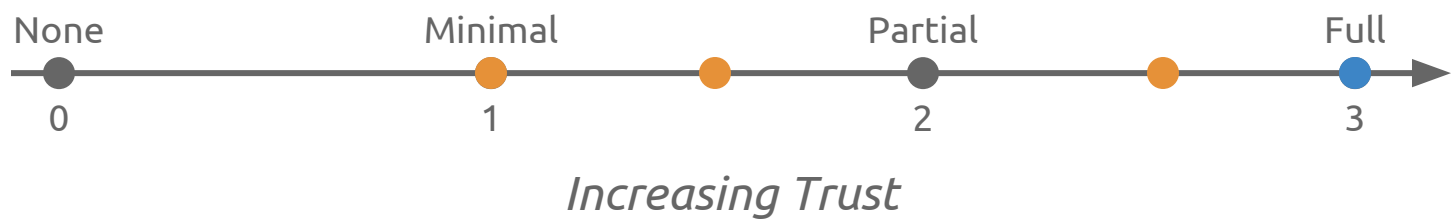
Application	Storage	Access	Manipulation	Meta-analysis	Score
Dropbox	Full	Full	Full	Full	12
Facebook	Full	Full	Full	Full	12
Gmail	Full	Full	Full	Full	12
Hangouts	Full	Full	Full	Full	12
Amazon EC2	Full	Full	Full	Full	12

Degree of Third Party Trust Across Capabilities



Application	Storage	Access	Manipulation	Meta-analysis	Score
Dropbox	Full	Full	Full	Full	12
Tresorit	Full	Partial	Partial	Full	10
Facebook	Full	Full	Full	Full	12
Gmail	Full	Full	Full	Full	12
PGP/GPG	Full	None	None	Full	6
Hangouts	Full	Full	Full	Full	12
TextSecure	Full	None	None	Minimal	4
LastPass	Full	Minimal	Full	Full	10
Amazon EC2	Full	Full	Full	Full	12

Degree of Third Party Trust Across Capabilities



Application	Storage	Access	Manipulation	Meta-analysis	Score
Dropbox	Full	Full	Full	Full	12
Tresorit	Full	Partial	Partial	Full	10
Facebook	Full	Full	Full	Full	12
Gmail	Full	Full	Full	Full	12
PGP/GPG	Full	None	None	Full	6
Hangouts	Full	Full	Full	Full	12
TextSecure	Full	None	None	Minimal	4
LastPass	Full	Minimal	Full	Full	10
Amazon EC2	Full	Full	Full	Full	12
Single SSP	Full	Partial	Partial	Full	10
Multiple SSPs	Partial	Minimal	Minimal	Partial	6

Degree of Third Party Trust Across Capabilities



Application	Implicit	Compelled	Unintended	Colluding	Score

Risk of Third Party Trust Violations



Application	Implicit	Compelled	Unintended	Colluding	Score
Dropbox	Disincent.	Known	Disincent.	N/A	5
Facebook	Known	Known	Disincent.	N/A	7
Gmail	Vulnerable	Known	Disincent.	N/A	6
Hangouts	Vulnerable	Known	Disincent.	N/A	6
Amazon EC2	Disincent.	Known	Disincent.	N/A	5

### Risk of Third Party Trust Violations



Application	Implicit	Compelled	Unintended	Colluding	Score
Dropbox	Disincent.	Known	Disincent.	N/A	5
Tresorit	Disincent.	Vulnerable	Disincent.	N/A	4
Facebook	Known	Known	Disincent.	N/A	7
Gmail	Vulnerable	Known	Disincent.	N/A	6
PGP/GPG	Disincent.	Disincent.	Minimized	N/A	2
Hangouts	Vulnerable	Known	Disincent.	N/A	6
TextSecure	Disincent.	Disincent.	Minimized	N/A	2
LastPass	Disincent.	Vulnerable	Disincent.	N/A	4
Amazon EC2	Disincent.	Known	Disincent.	N/A	5

### Risk of Third Party Trust Violations



Application	Implicit	Compelled	Unintended	Colluding	Score
Dropbox	Disincent.	Known	Disincent.	N/A	5
Tresorit	Disincent.	Vulnerable	Disincent.	N/A	4
Facebook	Known	Known	Disincent.	N/A	7
Gmail	Vulnerable	Known	Disincent.	N/A	6
PGP/GPG	Disincent.	Disincent.	Minimized	N/A	2
Hangouts	Vulnerable	Known	Disincent.	N/A	6
TextSecure	Disincent.	Disincent.	Minimized	N/A	2
LastPass	Disincent.	Vulnerable	Disincent.	N/A	4
Amazon EC2	Disincent.	Known	Disincent.	N/A	5
Single SSP	Disincent.	Disincent.	Minimized	Disincent.	3
Multiple SSPs	Disincent.	Minimized	Minimized	Minimized	1

### Risk of Third Party Trust Violations

