



Policy options for data privacy and protection

Roslyn Layton, PhD | Mar 2019



STRAND^{CONSULT}

Very Different Things

Data Security

Availability and confidentiality of data, securing against destruction and unauthorized access

Technical issue

Techniques to guard data

Data Protection

Mechanisms to recover data in the event of loss or destruction

Technical issue

Techniques to recover data

Data Privacy


Use and control of data, how people allowed to have data should use it

Legal issue

Principles and practices


How to Promote Trust Online

Business
Practices + Institutions



- Focus of GDPR, CCPA
- Empowers regulators and litigants
- Normative (whether and how to protect privacy)

User
Knowledge + Level/Type
Technology



- No focus in GDPR, CCPA
 - Empowers consumers and innovators
- Empirical (understanding behavior through experiments)

General Data Protection Regulation vs. California Consumer Privacy Act

GDPR

Word “privacy” appears once in statute (in footnote), EU: “data processing for mankind”, “global gold standard”

173 recitals

- 45 regulations on business practices
- 43 conditions of applicability
- 35 bureaucratic obligations
- 17 legal rights
- 11 administrative clarifications
- 9 policy assertions
- 5 enumerated penalties

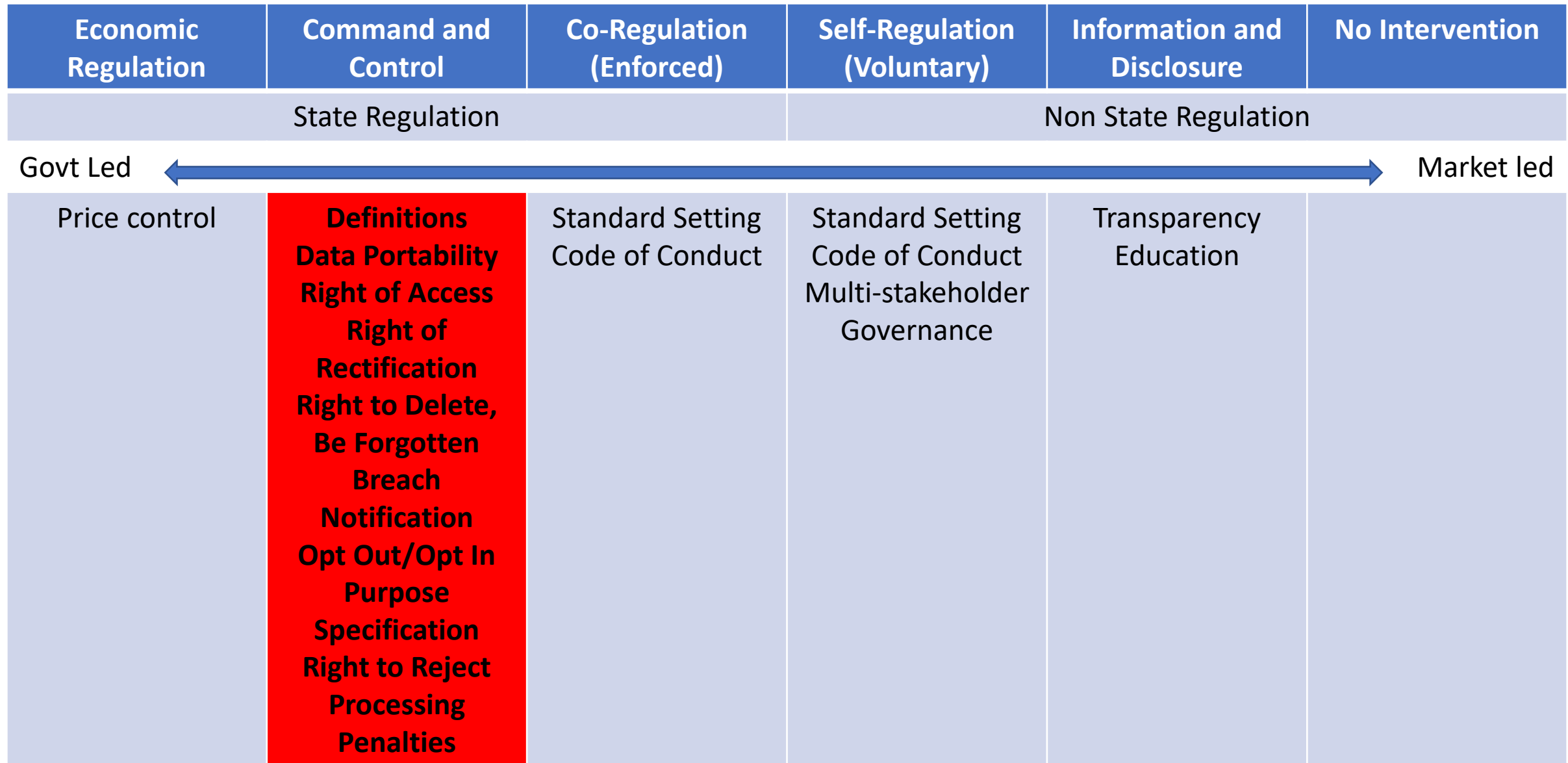
CCPA

Consumer rights are essentially regulations on data processing (natural vs. legal rights)

185 provisions

- 77 regulations on business practices
- 47 conditions of applicability
- 17 bureaucratic obligations
- 11 legal rights
- 17 administrative clarifications
- 6 policy assertions
- 10 enumerated penalties

Bills Don't Action Full Regulatory Continuum



Opposite Outcomes From GDPR Policymakers' Statements



Increased market share in Google, Facebook, Amazon



Decreased market share of EU ad tech firms



No improvement in consumer trust



Consumers deploy blockers on GDPR pop-ups



US media firms exited market



Automatic generation and gaming of complaints

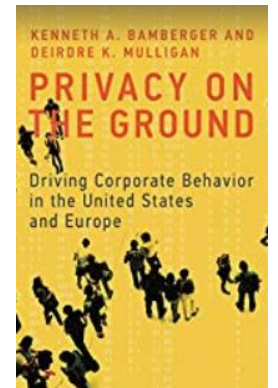
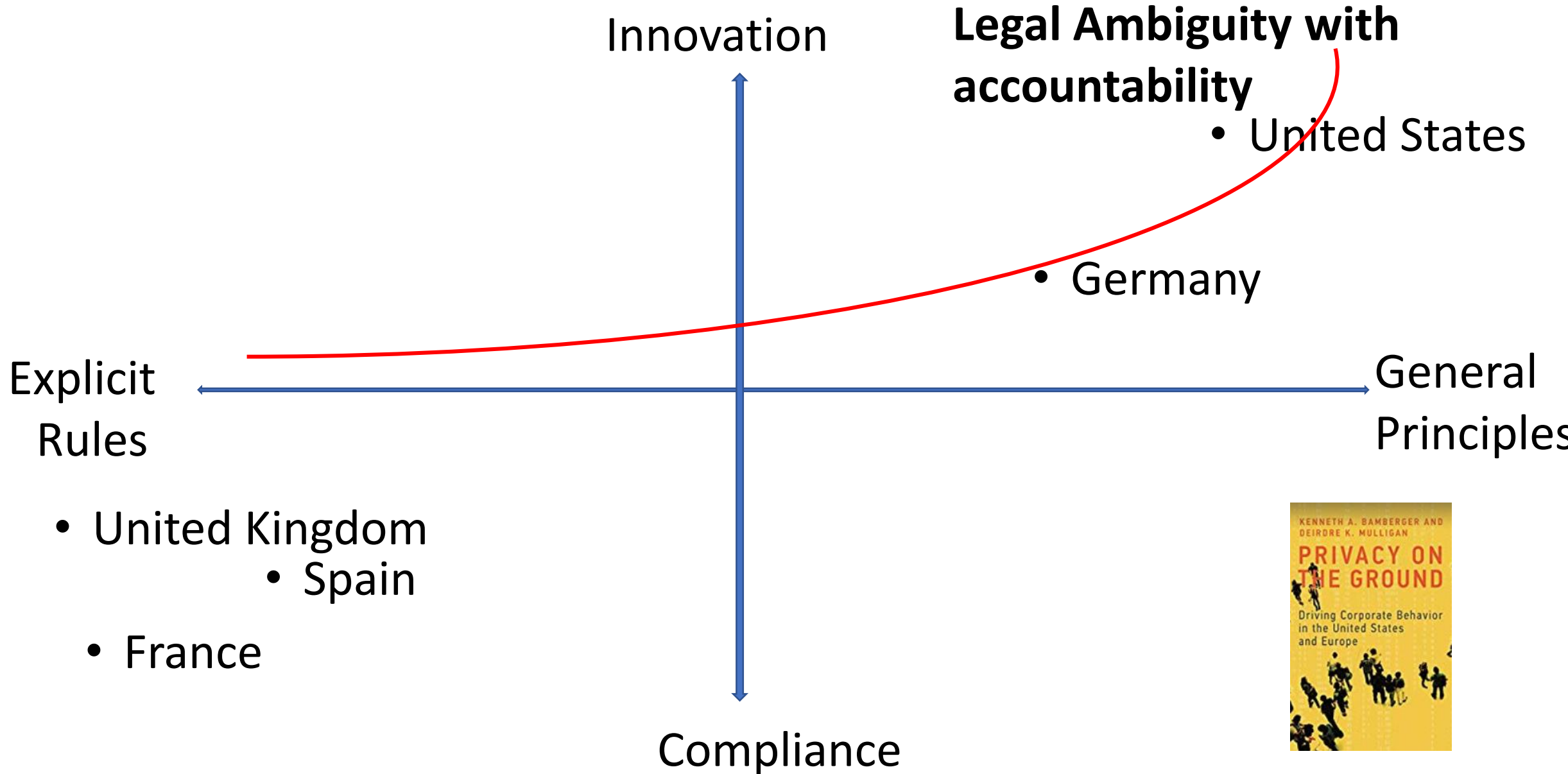


Most complaints are for telemarketing, emails, and video surveillance, not online platforms



WHOIS information not available to law enforcement, cybersecurity analysts, property rights holders

Historical Policy Outcomes for Data Protection



Data for USA



Americans concerned about privacy, though concern is falling. Greater concern about security, cybercrime etc. ([NTIA 2015, 2017](#)). Views differ by demographics (older may prefer more regulation, than younger)



Of Facebook users under 30, half switch off, one-third quit ([HH](#)), main reason is lack of time



Market value loss of FB following Cambridge is many times greater than GDPR fine ([CNBC](#))



Consumers don't object to data sharing, only inappropriate data sharing ([Nissenbaum](#))



Countries focused on principles rather than compliance make better privacy systems ([Privacy on the Ground, Bamberger/Mulligan](#))



Collective action of privacy advocates drove rules in EU and CA, not groundswell of public support

GDPR Compliance and Enforcement

- Ave firm spent \$1.3M to comply, need another \$1.8M expected (\$3M total). [\\$9B globally](#). Costs [being passed on](#) to customers, vendors, agencies as higher prices.
- Less than 50% of firms fully compliant. 20% say full compliance is impossible. ([IAPP](#))
- 14,000 new members to IAPP (now 44k members). 13,000 EU members.
- Complaints doubled to EU DPAs, data breach notifications tripled (many of these are coding errors) ([IAPP](#))
- 350 cases entered into EDPS system, about a dozen targeted for fines
- Likely 2 years before case resolution, pending litigation
- No funding to train regulators and data protection authorities



Privacy Enhancing Technologies (PETs)

Tools & Techniques

- Encryption
- Data minimization
- Authentication
- Attribute-based Access Controls
- Service-Level Agreements and Tools to Enable Transparency and Choice

Incentives

- NIST Guidelines
- Awards/prizes
- Privacy by design competitions, grants
- Safe harbors for good operators and experimentation
- Seals of Approval

Digital Competence Education

Curriculum Components

- Reputational harm
- Digital footprint
- Ads, Content Choice
- Online-Offline Balance
- Types of services
- Where your data goes
- Consent, disclosures
- Complaints, Remedies

Enablers

- Link to FTC and other privacy education tools on websites
- Rewards/discounts for customers to take online privacy training.
- Consumer-centric videos, cartoons etc.) to explain how their products and services, incorporate data.
- Task force of FTC, industry and consumers

Responsibilities of consumers

- Responsibility to be an educated consumer, including responsibility to gather and evaluate information before making a decision
- Responsibility to use products and services safely
- Responsibility to use information to make choices
- Responsibility to choose carefully
- Responsibility to express opinion about a product, as well as report improper business practices. This can be communicated to the community, firm, and/or authorities.
- Freedom to consume products and services that conform to one's values
- Expectation to consume without unfair, deceptive, and defective products and services and ability to seek redress from injury



Provisioning FTC for 21st Century

- Civil penalties
- Remove exemptions for common carriers, non-profits
- Narrowly-tailored rulemaking subjected to Congressional review
- Staffing: need economists, data scientists, and technologists (800 lawyers but 80 economists)
- Suggested 25 in enforcement, 25 in technology—however this should be coupled with analysis of expected investigations, enforcements, fines etc
- Presently 612 FTE in Consumer Protection, \$171M yr (\$280k/FTE)
- Staff will likely need to be housed in new location

What good tech policy looks like

- ✓ Aligned with the law and goals
- ✓ Based on holistic quantitative and qualitative evidence
- ✓ Has a stated reason and proposed outcome
- ✓ Provides a framework for achieving the outcome
- ✓ Crisp and widely understood
- ✓ Creates value and benefits with measurable outcomes
- ✓ Monitored, evaluated and reviewed regularly