Understanding Privacy Policies: Content, Self-Regulation, and Markets

Florencia Marotta-Wurgler
NYU School of Law

BCCP Inaugural Conference
June 17, 2016

“Notice and Choice”

- Consumer information privacy in the U.S. is protected using a “notice and choice” model
  - Disclosure via privacy policies
  - Self-regulatory guidelines with FIPs created by FTC
  - Enforcement mechanisms: FTC Sec. 5 actions against unfair/deceptive practices; U.S.-E.U. SHA; threat of regulation
- How is this model working?
  - Some say well, some say not so
  - But we really don’t know, because there has been little systematic examination of current practices
  - This matters because new proposals also rely on self/co-regulation

Two Papers

- Paper 1: A large-sample study of privacy policies

  Content: What are the current information practices?

  Self-Regulation: Are firms embracing the current guidelines?

  Markets: Who complies more than others?

- Goals are to inform current regulatory debates, understand outcomes of current regime, and see how "market forces" are also shaping PPs

Two Papers

- Paper 2 (with Daniel Svirsky): An examination of changes in privacy policies over time

  Enforcement Actions: After an FTC action against a firm engaged in US-EU SHA violation, do other violating firms correct their behavior?

  Other Dynamics: How do policies change over time?

- Goal is to inform discussions on Privacy Shield

261 Privacy Policies

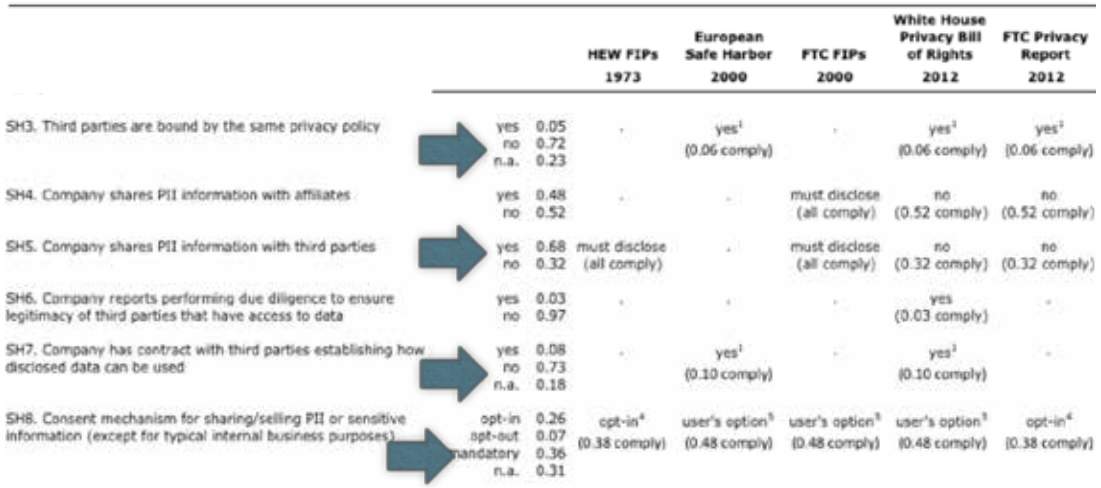
- Markets with various info. collection / sharing concerns
  - Adult
  - Cloud Computing
  - Dating
  - Gaming
  - News and Reviews
  - Social networks
  - Special Interest Message Boards
- From Google (#1) and Facebook (#2) to veggiedate.com (#278,952)
- Each policy graded on 49 dimensions noted in one or more prominent sets of privacy policy guidelines

Lots of Data Collection

Notice			HEW FIPs 1973	European Safe Harbor 2000	FTC FIPs 2000	White House Privacy Bill of Rights 2012	FTC Privacy Report 2012
N1. Policy is accessible through a direct link from the homepage	yes no n.a.	0.88 0.11 0.01	-	-	yes[1] (0.88 comply)	-	yes[1] (0.88 comply)
N2. Users asked to manifest consent when signing up via clickwrap	yes no n.a.	0.19 0.8 0.01	yes[1] (0.19 comply)	-	yes[1] (0.19 comply)	-	yes[1] (0.19 comply)
N3. Layered or short notice is presented	yes no	0.2 0.8	-	-	-	yes (0.2 comply)	-
N4. Contact data is collected and stored	yes no	0.96 0.04	must disclose (all comply)	-	must disclose (all comply)	-	-
N5. Computer data is collected and stored (e.g., IP address, browser type, OS)	yes no undisclosed	0.87 0.03 0.1	must disclose (0.90 comply)	-	must disclose (0.90 comply)	-	-
N6. Interactive data is collected and stored (e.g., browsing behavior or search history)	yes no undisclosed	0.71 0.13 0.16	must disclose (0.84 comply)	-	must disclose (0.84 comply)	-	-
N7. Financial information is collected and stored (e.g., account status or history, credit)	yes no n.a. undisclosed	0.47 0.23 0.03 0.27	must disclose (0.72 comply)	-	must disclose (0.72 comply)	-	must disclose (0.72 comply)
N8. Content is collected and stored (e.g., personal communications, stored documents, media)	yes no undisclosed	0.4 0.19 0.41	must disclose (0.59 comply)	-	must disclose (0.59 comply)	-	-
N9. Sensitive information is collected and stored (e.g., race, medical info, religion, sexual orientation, income, SSN)	yes no undisclosed	0.27 0.41 0.32	must disclose (0.68 comply)	-	must disclose (0.68 comply)	-	must disclose (0.68 comply)
N12. PII used internally only for business purposes (e.g., administering transaction, communication with user, research, internal database compilation, servicing site)	yes no	0.3 0.7	yes (.30 comply)	-	yes (.30 comply)	yes (.30 comply)	yes (.30 comply)
N13. PII used only for stated, context-specific purposes (e.g., user would expect that this data would be shared for service to function)	yes no n.a.	0.26 0.73 0.01	yes (.26 comply)	-	yes (.26 comply)	yes (.26 comply)	yes (.26 comply)
N14. Profile, picture, or other information may be used in advertising	yes no opt-in/opt-out	0.03 0.92 0.05	-	-	(no or) user's option (0.97 comply)	no (0.92 comply)	-
N15. Third parties may place advertisements that track user behavior	yes no undisclosed	0.62 0.14 0.24	-	-	no[2] (0.14-0.39 comply)	must disclose (0.76 comply)	no[2] (0.14-0.39 comply)

- Only 19% require explicit agreement
- Efforts to simplify policies have been ignored
- Few disclaim collection, not many impose limits
- Many just don't say (and no default rules)

Lots of Sharing



			HEW FIPs 1973	European Safe Harbor 2000	FTC FIPs 2000	White House Privacy Bill of Rights 2012	FTC Privacy Report 2012
SH3. Third parties are bound by the same privacy policy	yes	0.05	.	yes[1] (0.06 comply)	.	yes[1] (0.06 comply)	yes[1] (0.06 comply)
	no	0.72					
	n.a.	0.23					
SH4. Company shares PII information with affiliates	yes	0.48	.	.	must disclose (all comply)	no (0.52 comply)	no (0.52 comply)
	no	0.52					
SH5. Company shares PII information with third parties	yes	0.68	must disclose (all comply)	.	must disclose (all comply)	no (0.32 comply)	no (0.32 comply)
	no	0.32					
SH6. Company reports performing due diligence to ensure legitimacy of third parties that have access to data	yes	0.03	.	.	.	yes (0.03 comply)	.
	no	0.97					
SH7. Company has contract with third parties establishing how disclosed data can be used	yes	0.08	.	yes[1] (0.10 comply)	.	yes[1] (0.10 comply)	.
	no	0.73					
	n.a.	0.18					
SH8. Consent mechanism for sharing/selling PII or sensitive information (except for typical internal business purposes)	opt-in	0.26	opt-in[4] (0.38 comply)	user's option[5] (0.48 comply)	user's option[5] (0.48 comply)	user's option[5] (0.48 comply)	opt-in[4] (0.38 comply)
	opt-out	0.07					
	mandatory	0.36					
	n.a.	0.31					

- Third parties, “affiliates”
- But they are rarely bound by same policy—and perhaps by no contract
- User often has no choice

Intermediaries and Seals?

- Fine print is unlikely to be read …
  - Bakos, Marotta-Wurgler, Trossen 2014
- Seals and third party certifications could help, but
  - Only 29.5% adopt a third party seal (e.g., TRUSTe, BBB Online) or *claim* to adhere to a safe harbor agreement
  - Most of those who claim adherence to SHA have numerous terms that run counter to its requirements
- Machine learning techniques also hard to implement due to internal contradictions and inconsistencies in writing

Compliance with FTC 2012

	All N = 261	Adult N = 17	Cloud Computing N = 28	Dating N = 40	Gaming N = 20	News and Reviews N = 18	Social Networks N = 89	Special Interest Message Board N = 49
Panel A. Compliance								
OVERALL	0.39	0.53	0.45	0.38	0.34	0.38	0.38	0.34
Notice	0.45	0.68	0.44	0.46	0.41	0.5	0.44	0.41
Sharing	0.37	0.68	0.39	0.35	0.19	0.33	0.34	0.43
User Control	0.64	0.53	0.71	0.75	0.65	0.61	0.69	0.46
Security	0.42	0.51	0.63	0.39	0.41	0.41	0.41	0.33
Data Practices	0.04	0.03	0.02	0.01	0.03	0	0.07	0.03
Enforcement	0.42	0.47	0.61	0.48	0.3	0.39	0.37	0.39
Privacy by Design	0.13	0.06	0.43	0.03	0.15	0.06	0.16	0.04

Qualifications

- Can measure only what firms say, not what they do
  - Could be better, could be worse
  - But firms may face FTC and state actions if mislead
  - Regulators also make decisions based on what they can see
- Always hard to say whether current practices are “optimal”
  - But knowing what they are should help inform policymakers
- Hard to disentangle variation in policies between guidelines, market forces, and other factors

Changes Over Time

- A subset of previous sample
  - Weekly snapshots of 251 PPs from July 2010-July 2013
- Each policy graded on 26 further dimensions (75 terms total)
  - Including SHA compliance

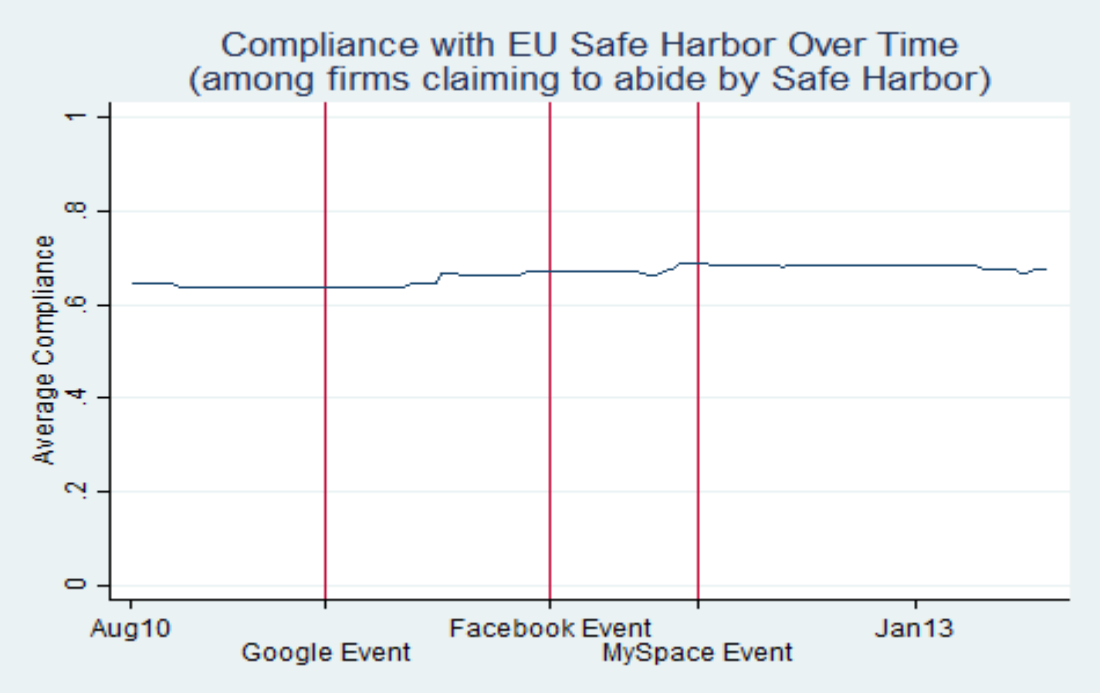
Events

- We focus on enforcement actions brought during the sample period that target the content of PPs
  - Four events targeting SHA violations
    - Note that firms claiming SHA enter sample with low compliance
- Look at other term changes over the sample period
  - Do firms reduce the number of actionable promises?

Events

Event	Action	Dates	Allegation in FTC Complaint (pincite)	Terms of interest
1	American Apparel, Inc. FTC No. 142-3036, et al.	Jan. 21, 2014 (PR) May 9, 2014 (CO) June 25, 2014 (S)	American Apparel "did not renew its self-certification to the Safe Harbor Frameworks" but "certified that it abides by the Safe Harbor privacy principles." (11-12)	Does firm claim EU Safe Harbor certification? Is it in fact registered?
2	Google, Inc., FTC No. 102-3136	Mar. 30, 2011 (PR) Oct. 13, 2012 (CO) Oct. 21, 2012 (S)	Google's privacy policy claimed to "'adhere[] to the US Safe Harbor Privacy Principles.'" (7). In fact, because Google shared personal information without notice, the claims regarding EU Safe Harbor "were, and are, false or misleading." (8)	If firm claims EU Safe Harbor compliance, does the privacy policy comply with EU Safe Harbor requirements for privacy policies?
3	MySpace, LLC., FTC No. 102-3058	May 8, 2012 (PR) August 30, 2012 (CO) September 11, 2012 (S)	Myspace claimed that it "'complies with the U.S.-EU Safe Harbor Framework.'" (7), but in fact shared customers' personal information with advertisers (3) without notice or consent (4).	If firm claims EU Safe Harbor compliance, does the privacy policy comply with EU Safe Harbor requirements for privacy policies?
4	Facebook, Inc., FTC No. 092-3184	Nov. 29, 2011 (PR) Aug. 10, 2012 (S)	"Facebook retroactively applied…changes to personal information that it had previously collected from users, without their informed consent" (9).	If firm claims EU Safe Harbor compliance, does the privacy policy comply with EU Safe Harbor requirements for privacy policies?

Google, Facebook, MySpace



Google, Facebook, MySpace

Same results for other measures of compliance; within markets; and for changes in compliance of targeted terms

A Perverse Effect of Deception?

- Can't prove a causal connection
- Firms have been dropping data security promises
  - 10% removed promise related to data security; 5% removed promises related to managerial safeguards of data; statistically significant
- Slight improvement in terms brought under Unfairness
  - Retroactive changes; Indefinite data retention periods
  - (More notices information sharing with Government after Snowden)

Qualifications

- Can't observe what firms do, just what they say in PP
  - Could be better, could be worse; but a large fraction deception claims focus on privacy policy statements
- Behavior might improve in ways not reflected in PPs
  - But why won't firms update when doing so affects compliance?
- Generalizability
  - But hard to imagine firms will ignore actions against Facebook or Google and focus on smaller ones
  - SHA actions mostly tagged to other violations

Conclusions

- First large-sample analysis of privacy policies
- Current regulatory model appears to be having relatively limited impact on privacy policies
  - Compliance with guidelines is modest by any measure
  - Little change in compliance after SHA enforcement actions
  - If real impact is elsewhere, maybe focus on PPs is misguided
- Market forces may be playing a role; can see some intuitive differences in PPs across firms

Figure 1. Compliance With FTC 2012 Guidelines