

Does Law Matter? Information Privacy and Online Compliance in Israeli Websites

Michael Birnhack & Niva Elkin-Koren

Tel-Aviv University

Haifa University

CIPLIT, October 2009

ISF Grant 867/04

Overview

- **In a nutshell:**
 - research examined compliance of Israeli websites to legal requirements and their overall privacy practices
 - Empirical legal study & security evaluation
- The purpose of the study
- Methodology
- Findings
- Ramifications

Purpose & Frames

The Frameworks

- **Informational privacy debate**
 - Should we regulate?
 - How to regulate?
 - Consent? Choice?
- **Online regulation**
 - Can law regulate online activity?
 - Forms of regulation (public / private)
 - What else is going on?
- **Law in the books, law in action**
- **Empirical legal study**

Methodology

The Study

- **Legal Analysis**
 - Do the information practices trigger the legal duties?
 - If yes: compliance? esp. notice
- **Information practices**
 - Over-compliance?
- **Actual practices**
 - Is there a gap between stated policy and actual practices?

The Dataset

- **Formal test** – ccTLD <.il>
- www.buy.co.il
- But not:
 - www.buy.co.il/cars
 - www.cars.buy.co.il

● **Prior research**

- Birnhack & Elkin-Koren '03: compliance of Public Websites

● **Current research**

- Public websites
- Commercial and NGO websites
- Popular websites
- Sensitive websites

Dataset

	Definition	Selection	Total
Public Sector	gov.il, muni.il, ac.il, k12.il, net.il	The entire population	289/497
Private Sector	co.il	A Representative sample of randomly selected websites	726/1000
	org.il	A Representative sample of randomly selected websites	190/250
Popular		Phone Survey	45
Sensitive		Content-based Selection	118
	Filtering out: overlaps, inactive, cross-linked		1368

Israeli Data Protection Law

- Comprehensive data protection regime, EU style
- Constitutional right + Privacy Protection Act

1. Data collectors: duties

2. Data Subjects Rights

3. Enforcement

- Administrative, criminal, civil

- EU “adequacy assessment”
- Legislative amendments expected

Duties and Rights

Duties

- Registration (s.8)
- Notice (s. 11) indicating
 - legal duty to provide the information?
 - Purpose;
 - Onwards transfer? Purpose.
- Confidentiality (s. 16)
- Data security (s. 17)

Data Subjects' Rights

- access (s. 13)
- rectification (s. 14)
- rights correlative to duties
 - Civil cause of action (but hardly any)
 - Class action?

Questionnaire

- **Identify data collection**

- Kind of data (according to PPA)
 - Merely Contact Information is excluded
 - Personal data (PPA definitions)

- **Compliance**

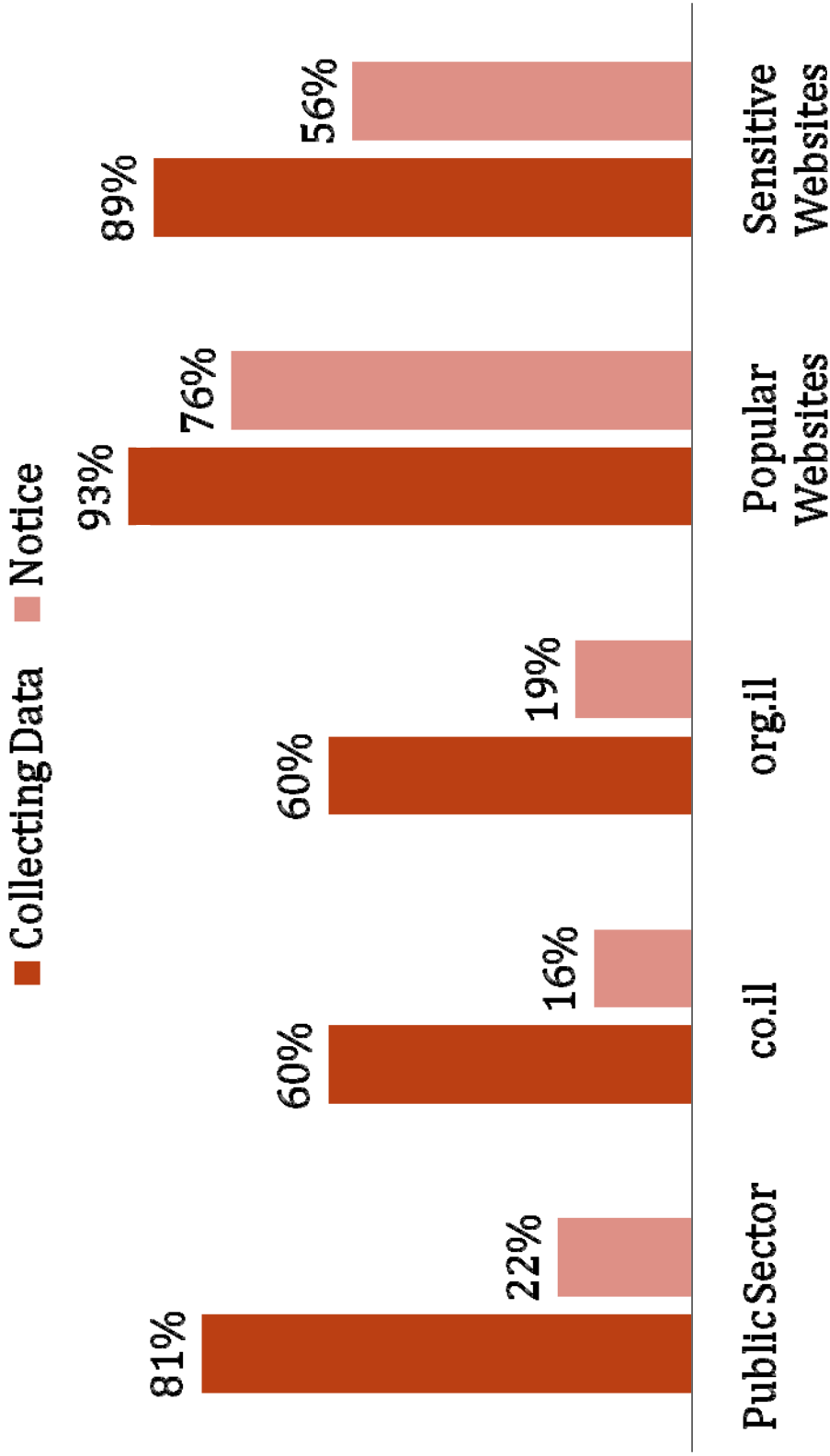
- “hard compliance” - notice requirement (s. 11)
- “soft compliance” - look and feel

Findings

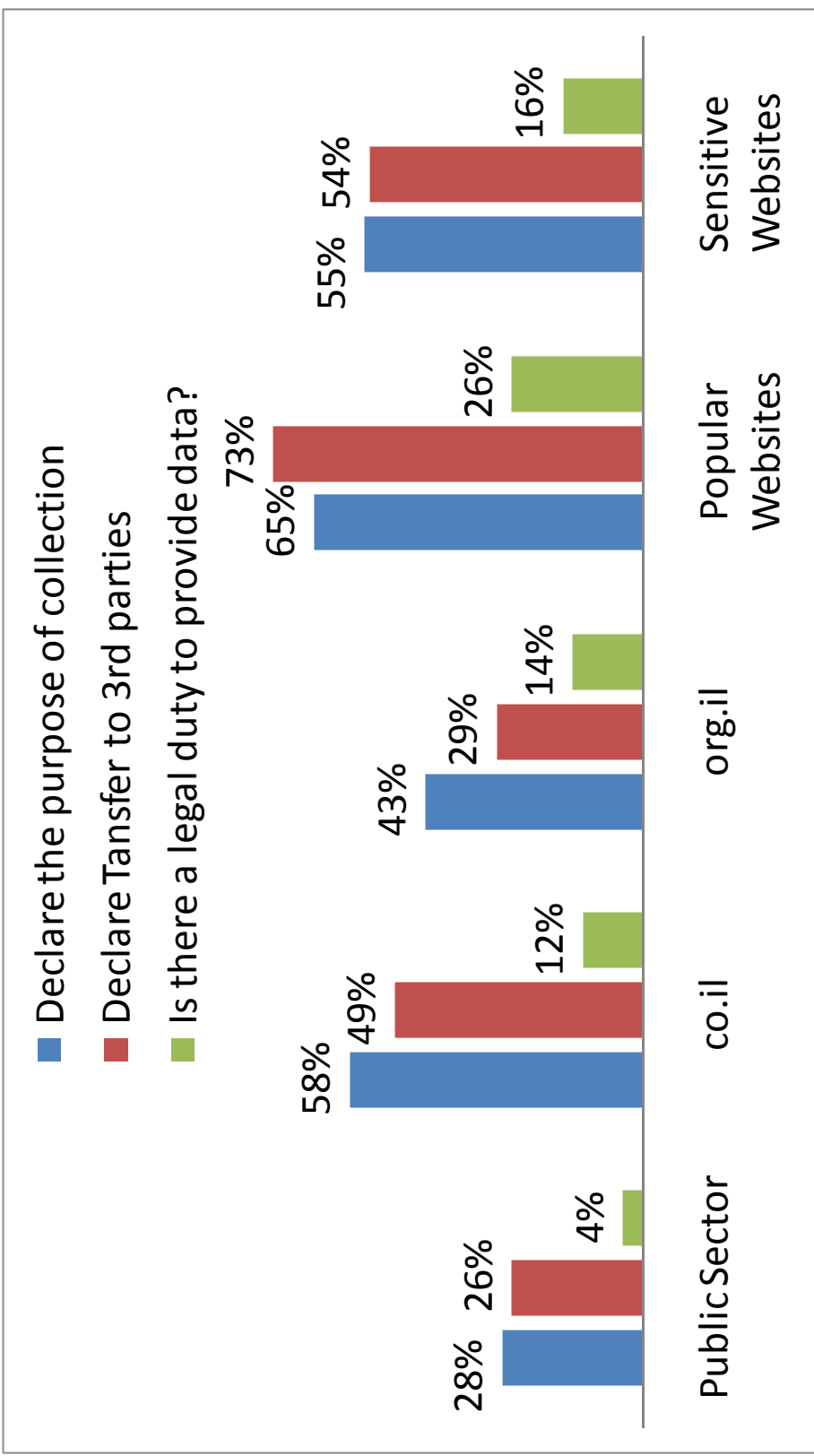
Personal data collection

Type of Websites	Websites collecting <u>data</u>	Websites requiring <u>identification</u>		Personal data required for obtaining a <u>username</u> or for <u>access</u>	feasibility of <u>false</u> personal data
		Of total websites	Of data collecting websites		
Public Websites	81%	50%	62%	13%	51%
Private Sector	co.il	56%	93%	13%	85%
	org.il	45%	75%	8%	59%
Popular	93%	84%	86%	53%	67%
Sensitive	89%	84%	94%	49%	71%

Hard Compliance



Hard Compliance: A closer look



Soft Compliance: Look & Feel

Low visibility of Notice in all sectors

- Heading of notice
- Visibility of links to notice
- Location of links
- Links reliability
- Prominence of links

Over-compliance

- **Access & Rectification**
 - No duty to notify data subjects of their right
 - Yet, a notice in 24% of Popular but only 7% of Public
- **Data Security**
 - A duty to provide data security
 - No duty to announce it
 - Yet, a large number of websites post a statement on data security

Data Security

Type of Websites	Data Security Statement (not mandatory)	Detailed Statement (% of those which have a data security statement)
Public Websites	24%	24%
Private Sector	co.il	50%
	org.il	44%
Popular Websites	55%	29%
Sensitive Websites	58%	34%

Actual practices

- **Tested in Sensitive Websites**
 - Data security
 - Use of cookies
 - Third-party cookies
 - External applications
 - Whether security failures were detected
- **Findings**
 - 58% data security statement
 - But, only 10% actually provided data security

Ramifications

Some Conclusions

- The State is still a major threat to privacy
 - Non-compliance among Public Websites
 - Failure of Notice
 - Better level of compliance among large commercial websites (popular, sensitive)
 - Other forces at play (market forces?)
 - Less effective among small businesses and NGOs
 - Might be irrelevant for threat to privacy in the Web 2.0 environment

Policy Conclusions

- Law:
- First Order regulation:
 - Amend notice requirement
 - Better enforcement
 - Internalize legal requirements
- Second Order regulation:
 - Visibility?
 - Transparency?
 - Default rules?
 - Require “privacy officers”?
- Or, get rid of the law?

Thanks!

Michael birnhack@post.tau.ac.il

Niva elkiniva@law.haifa.ac.il