Chapter 14:
Customer Privacy Concerns and Privacy Protective Responses
Overview

Topics discussed:

- The Concept of Customer Privacy
- Drivers of Customer Privacy Concerns
- Regulations to Protect Customer Privacy
- Customer Privacy Protective Responses
- Privacy Paradox
- Consequences of Customer Privacy Protective Responses
- Implications for Companies
The Concept of Customer Privacy

Customer privacy can be defined as “the power of the individual to personally control (vis-à-vis other individuals, groups, organizations, etc.) information about one’s self.”

The includes control over the collection, storage, usage, and release of personal information.

Stone, Gueutal, Gardner, & McClure, 1983
For successful CRM, the firm must ensure a constant flow of up-to-date information about customers’ buying habits and individual needs.

If customers feel they are losing control over their personal information, they will begin to feel concern about their privacy.

CUSTOMER PRIVACY CONCERNS

Serious obstacles for the efficiency of a company’s CRM practices.
Two main drivers of customer privacy concerns:

- Internal, company-related drivers
- External drivers

Internal Drivers of Customer Privacy Concerns
- Collection
- Control
- Awareness
- Errors
- Improper Access
- Unauthorized Secondary Use

External Drivers of Customer Privacy Concerns
- Internet
- Technology
- Public Media
- Governmental Regulations

Customer Privacy Concerns

Malhotra, Kim, & Agarwal, 2004
Internal Drivers of Customer Privacy Concerns

- **Collection** – Amount and way in which personal information is collected
- **Control** – Degree of control over personal information
- **Awareness** – Understanding of established conditions and actual practices
- **Errors** – Protections against errors in personal information
- **Improper Access** – Access of unauthorized parties to personal information
- **Unauthorized** – Usage of personal information for unauthorized purposes
  **Secondary Use**

Malhotra, Kim, & Agarwal, 2004
External Drivers of Customer Privacy Concerns

- Internet
- Technology
- Public Media
- Governmental Regulations
External Drivers of Customer Privacy Concerns – Internet

Ways to collect customer information online:

- Customers voluntarily enter personal information, such as their name, address, and credit card number, into databases.
- Information on customers’ online behavior is collected using cookies and click-stream technology **without customers’ consent**.

CUSTOMER PRIVACY CONCERNS

- 68% of U.S. customers “definitely” would not allow companies to track their online behavior to tailor advertisements to their interest, i.e., behavioral advertising.

Turow, King, Hoofnagle, Bleakley, & Hennessy, 2009
External Drivers of Customer Privacy Concerns – Technology

- **Mobile and smart phones (esp. location-based services)**
  - Eroding distinction between public and private space
  - Risk of oversharin (see Pleaserobme-example)

- **Radio frequency identification technology**
  - Action threat – Track customer behavior without consent (see Broken Arrow Affair)
  - Association threat – Create comprehensive customer profiles by liking the customer with the tagged item (infer brand or item preferences)
  - Location threat – Create comprehensive customer profiles by liking the customer with the tagged item (infer brand or item preferences)
External Drivers of Customer Privacy Concerns – Public Media

- Increased media coverage of customer privacy issues since 1990
  - Total no. of articles increased by 70%
  - Three times more negative than positive articles

Roznowski, 2003
External Drivers of Customer Privacy Concerns – Governmental Regulations

- Perceived lack of business policy or governmental regulation
- Extent to which governments (mis)use personal information

CUSTOMER PRIVACY CONCERNS

- European Constitutional Report 2010
  - Does a constitution exist and does it protect privacy?
  - Are there other protections, e.g., rights to data protection and private communication?

Wirtz, Lwin, & Williams, 2007, privacyinternational.org, 2010
Regulations to Protect Customer Privacy

Customer Privacy Regulations

- Industry self-regulation
  - Example: USA

- Government-imposed regulation
  - Example: Germany
Regulations to Protect Customer Privacy

- **U.S. Constitution** → Limited constitutional right of privacy (Bill of rights)
- **Robinson list** → Do-Not-Call registry to avoid receiving telemarketing call
- **Federal Trade Commission (FTC)** → Main agency protecting U.S. customers privacy
  - Fair Information Practice Principles
    - Notice and Awareness
    - Choice and Consent
    - Access
    - Integrity and Security
    - Enforcement and Redress
  - “The industry must do better. For every business, privacy should be a basic consideration – similar to keeping track of costs and revenues, or strategic planning.” (FTC, 2000)
  - Enforcement through legal settlements (see Google buzz case)
Regulations to Protect Customer Privacy

- **German Constitution** → “Privacy letters, posts, and telecommunication shall be inviolable.” (Article 10 of the Basic Law)

- **Data Protection Law** → General purpose = protect individual rights to avoid impaired privacy
  → The act covers the collection, processing, and use of personal data by public federal authorities and state administrations and by private bodies that rely on data processing systems or non-automated filing systems for commercial or professional use.

- **The Teleservices Data Privacy Act** → The act protects customer privacy online and requires explicit user consent before the usage logs of a session may be stored.

- **Section 7 of the Unfair Competition Act** → It is unfair to annoy customers inappropriately. This rules applies to unwanted advertisements, unsolicited commercials phone calls, marketing methods that use automated calling machines, fax machines or email (spam) received without prior consent, and any direct marketing that cannot be linked to the senders’ identity.
## Regulations to Protect Customer Privacy

<table>
<thead>
<tr>
<th>Feature</th>
<th>U.S.</th>
<th>Germany</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cold calling</td>
<td>Allowed (if not on Robinson List)</td>
<td>Forbidden</td>
</tr>
<tr>
<td>Contacting prospective clients or customers with unexpected telephone calls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unsolicited commercial e-mails</td>
<td>Forbidden</td>
<td>Forbidden</td>
</tr>
<tr>
<td>Commercial electronic messages, typically sent out in bulk without any prior request or consent given by the consumer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cross-country data transfer (U.S. to Germany and vice versa)</td>
<td>Allowed</td>
<td>Only allowed with Safe Harbor compliance</td>
</tr>
<tr>
<td>Transfer of customer-related data to a different country than where it has been collected, such as when consumers make online purchases from sellers located in a different country</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data transfer to third parties (without consent)</td>
<td>Allowed</td>
<td>Forbidden</td>
</tr>
<tr>
<td>Provision of personal data to other companies, such as marketing service providers, without notifying the customer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Right to opt-out from data collection</td>
<td>Not given</td>
<td>Given</td>
</tr>
<tr>
<td>Upon providing their personal information, customers are able to deny any further use of their data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Regulations to Protect Customer Privacy

Safe Harbor Provisions

- Agreement between the U.S. Department of Commerce and the European Commission
- Goal = Minimum level of protection for data of European origin.

**Key Principals:**

1. Notice – Customer notification about purpose and usage of their data
2. Choice – Opportunity to choose whether or not to disclose their data to third parties
3. Onward transfer of data – Data transfer only possible to companies complying with Safe Harbor
4. Access – Opportunity to access data for amendments and deletion
5. Security – Data protection from loss, any unauthorized access, disclosure, alteration, and destruction
6. Data integrity – Affirmation of data relevance, reliability, accuracy, completeness, and currentness for the purpose of usage
7. Enforcement – Mainly by industry self-regulation, supported by governmental enforcement activities (e.g., FTC)
Customer Privacy Protective Responses

1. Customer Privacy Concerns
   - Privacy Protective Responses
     - Information Provision
       - Refusal
       - Misrepresentation
     - Private Action
       - Removal
     - Public Action
       - Word of Mouth
       - Complaining directly to Companies
       - Complaining directly to Third Party

Based on Son and Kim, 2008
Customer Privacy Protective Responses

- Information Provision
  - Refusal – Refusal to give out information
  - Misrepresentation – Disclosure of falsified information

- Private Action
  - Removal – Information boycotts, removal of information
  - Word-of-Mouth – Voicing negative comments to friends/relatives

- Public Action
  - Complaining directly to Companies – Opportunity for companies to solve the issue
  - Complaining directly to Third Party – Large audience, organizations include EPIC and FTC

Son and Kim, 2008
Privacy Paradox

The privacy paradox can be explained as the “relationship between individuals’ intentions to disclose personal information and their actual personal information disclosure behaviors.”

Norberg, Horne & Horne, 2007

54% of Internet users believe that websites that tracked their behavior invaded their privacy.

But 64% of them would offer personal information to access a website.

Norberg, Horne & Horne, 2007
Consequences of Privacy Protective Responses

Customer Privacy Concerns

Customer Privacy Protective Responses

Loss of Trust and Brand Integrity

Decreased Sales

Decreased in Data Quality

Increased costs due to privacy protection

Ethical dilemma

Blattberg, Kim, & Neslin, 2008
Consequences of Privacy Protective Responses

Customer Privacy Concerns

Customer Privacy Protective Responses

Consequences of Privacy Protective Responses

Blattberg, Kim, & Neslin, 2008
Implications for Companies

- **Align privacy with strategy**
  - Take a lead in customer privacy protection
  - Especially important for companies with valuable brands

- **Look beyond rules to values**
  - Incorporate privacy and security values into corporate culture
  - Establish a set of comprehensive rules

- **Anticipate issues**
  - Create a position for a privacy officer or the alike
  - Scan for products and practices that raise legitimate privacy concerns
  - Collaborate with stakeholders to develop reasonable solutions

- **Create accountability**
  - Clarify responsibilities

- **Rely on technology when appropriate**
  - Simple tools can assist in privacy protection compliance
Implications for Companies

- **Do not conflate security and privacy**
  - Comply with societal and regulatory expectations with respect to the type of data, data protection, and the alike.
  - Be aware of different legal requirements in different countries

- **Treat privacy as a social responsibility**
  - In globally connected, information-rich societies, privacy and data protection belong on the corporate citizenship agenda

- **Manage your data supply chain**
  - International business need standards for data management that applies to expectations and regulations in an international context

- **Plan for disaster recovery**
  - In case of a data loss or breach, a rehearsal response should be in place

- **Heed both boomers and millennials**
  - Privacy thinking should span generational norms

Pearson, 2007
Customer privacy is driven by internal as well as external factors.

Internal drivers advert to company-related operations which evoke customers’ fears about disclosure and handling of their personal information.

The Internet, technological advances, public media coverage, and governmental regulations present the external drivers of customer privacy.

Privacy protection in the U.S. in based on industry self-regulation. One central role is hereby occupied by the FTC.

Germany as a member of the E.U. protects privacy by different governmental laws and regulations. For example, cold calling is not allowed without prior consent.

The Safe Harbor provision provides guidelines for the proper collection and handling of customer data for multinational U.S. companies operating in the E.U.

Customers’ privacy protective responses, namely information provision, private action, and public actions, can have serious ramifications for companies.

Customers’ intention to respond to privacy concerns do not always translate into actual behavior (privacy paradox).