

# Privacy and Information Security Law

Randy Canis

CLASS 6

**Consumer Data pt. 1**

## Privacy Policies

- Part of self-regulation
- “[Privacy] policies describe the information that is collected, how it will be used and shared, and how it will be safeguarded. Consumers are sometimes offered a choice to opt-out of some uses of their data.”

2

---

---

---

---

---

---

---

---

## FTC’s View

- “Since the late 1990s, the Federal Trade Commission (FTC) has deemed **violations of privacy policies to be an ‘unfair or deceptive’ practice under the FTC Act**. The FTC has the power to enforce the FTC Act. The result of the FTC’s involvement has been to create a system of quasi-self-regulation, where **companies define the substantive terms** of how they will collect, use, and disclose personal data, but they are then **held accountable to these terms by the FTC**. Over time, however, the FTC has interpreted the FTC Act as requiring more of companies than merely following promises.”

3

---

---

---

---

---

---

---

---

## Compliance and Strategy

- “**Compliance** means developing safeguards, including training the workforce, to make sure that the company follows all privacy and security laws and regulations. **Strategic thinking** means assessing privacy risks, training the workforce about privacy awareness, helping to shape products and services so that they minimize any potential privacy concerns, and stopping or limiting a company’s actions that consumers might find too privacy-invasive.”

4

---

---

---

---

---

---

---

---

## Potentially Applicable Laws

- 1) Tort Law
- 2) Contract Law
- 3) Property Law
- 4) FTC Section 5 Enforcement
- 5) Federal Statutory Regulation
- 6) State Statutory Regulation

5

---

---

---

---

---

---

---

---

## FTC Section 5 Enforcement

- “Since the mid-1990s, the Federal Trade Commission (FTC) has used Section 5 of the FTC Act to regulate consumer privacy. Section 5 prohibits ‘unfair or deceptive acts or practices in or affecting commerce.’ 15 U.S.C. §45. The FTC views **violations of privacy policies as a ‘deceptive’ practice.**”

6

---

---

---

---

---

---

---

---

## Pineda v. Williams-Sonoma Stores

- Issue
  - Is §1747.08 of the Song-Beverly Credit Card Act of 1971 violated when a business requests and records a ZIP code in association with a credit card and uses the information ultimately for marketing purposes?
  - Is a ZIP code without more personal information under §1747.08?

7

---

---

---

---

---

---

---

---

## Pineda v. Williams-Sonoma Stores

- “The Song-Beverly Credit Card Act of 1971 (Credit Card Act) (Civ. Code, § 1747 et seq) is ‘designed to promote consumer protection.’ ... One of its provisions, section 1747.08, prohibits businesses from requesting that cardholders provide ‘personal identification information’ during credit card transactions, and then recording that information.”

8

---

---

---

---

---

---

---

---

## Pineda v. Williams-Sonoma Stores

- How was the information collected?
  - “She then went to the cashier to pay for the item with her credit card. The **cashier asked plaintiff for her ZIP code** and, believing she was required to provide the requested information to complete the transaction, plaintiff provided it. The cashier entered plaintiff’s ZIP code into the electronic cash register and then completed the transaction. At the end of the transaction, defendant had plaintiff’s credit card number, name, and ZIP code recorded in its database.”

9

---

---

---

---

---

---

---

---

## Pineda v. Williams-Sonoma Stores

- How was the information used?
  - “Defendant subsequently used customized computer software to perform **reverse searches** from databases that contain millions of names, e-mail addresses, telephone numbers, and street addresses, and that are indexed in a manner resembling a reverse telephone book. The software **matched plaintiff’s name and ZIP code with plaintiff’s previously undisclosed address**, giving defendant the information, which it now **maintains in its own database**. Defendant uses its database to **market products** to customers and may also **sell the information** it has compiled to other businesses.”

10

---

---

---

---

---

---

---

---

## Pineda v. Williams-Sonoma Stores

- Section 1747.08, subdivision (a) provides, in pertinent part, “[N]o person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business shall . . . : (2) **Request, or require as a condition to accepting the credit card** as payment in full or in part for goods or services, the cardholder to provide **personal identification information**, which the person, firm, partnership, association, or corporation accepting the credit card writes, causes to be written, or otherwise records upon the credit card transaction form or otherwise. Subdivision (b) defines personal identification information as “information concerning the cardholder, **other than information set forth on the credit card**, and including, but not limited to, the cardholder’s address and telephone number.”

11

---

---

---

---

---

---

---

---

## Pineda v. Williams-Sonoma Stores

- Does a partial address count?
  - “a ZIP code is readily understood to be part of an address; when one addresses a letter to another person, a ZIP code is always included. The question then is whether the Legislature, by providing that “personal identification information” includes “the cardholder’s address” intended to include components of the address. The answer must be yes.”

12

---

---

---

---

---

---

---

---

## Apple v. Krescent

- Issue
  - Does section 1747.08 prohibits an online retailer from requesting or requiring personal identification information from a customer as a condition to accepting a credit card as payment for an electronically downloadable product?

13

---

---

---

---

---

---

---

---

## Apple v. Krescent

- “[T]he Legislature ‘sought to address the misuse of personal identification information for, inter alia, marketing purposes, and found that there would be no legitimate need to obtain such information from credit card customers if it was not necessary to the completion of the credit card transaction.’”

14

---

---

---

---

---

---

---

---

## Apple v. Krescent

- What are key differences of online retailers versus brick and mortar retailers?

15

---

---

---

---

---

---

---

---

## Apple v. Krescent

- Holding
  - “[S]ection 1747.08 **does not apply** to online purchases in which the product is downloaded electronically.”

16

---

---

---

---

---

---

---

---

## Other Use of Email Address

- “[A] federal court found that Nordstrom violated the act by requesting an e-mail address to mail a customer a receipt and then also using the e-mail to send the customer promotional communications and materials.”

17

---

---

---

---

---

---

---

---

## Injury and Standing Requirement

- “In federal courts, in order to have **standing**, the plaintiff ... must show that (1) it has suffered an ‘injury in fact’ that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.”

18

---

---

---

---

---

---

---

---

## In re Google, Inc.

- Issue
  - Could Google properly adopt is universal privacy policy allowing for combination of a user’s personal identification information (PII) across multiple Google products?

19

---

---

---

---

---

---

---

---

## In re Google, Inc.

- What PII may be combined?
  - first and last name; home or other physical address (including street name and city); current, physical location, a user's email address, and other online contact information (such as the identifier or screen name); IP address; telephone number (both home and mobile numbers); list of contacts; search history from Google's search engine; web surfing history from cookies placed on the computer; and posts on Google+

20

---

---

---

---

---

---

---

---

## In re Google, Inc.

- "Plaintiffs contend that Google's new policy violates its prior policies because the new policy no longer **allows users to keep information gathered from one Google product separate** from information gathered from other Google products. Plaintiffs further contend that Google's new policy violates users' privacy rights by allowing Google to **take information** from a user's Gmail account, for which users may have one **expectation of privacy**, for use in a **different context**, such as to personalize Google search engine results, or to personalize advertisements shown while a user is surfing the internet, products for which a user may have an entirely different expectation of privacy. In addition to commingling Plaintiffs' PII across the various Google products, Plaintiff contend Google has **shared Plaintiffs' PII with third-party entities** who have partnered with Google in order to develop applications for the Google Play app store to help it place targeted advertisements."

21

---

---

---

---

---

---

---

---

## In re Google, Inc.

- "To satisfy Article III, a plaintiff 'must show that (1) it has suffered an "injury in fact" that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.'"

22

---

---

---

---

---

---

---

---



## In re Google, Inc.

- “[I]njury-in-fact in this context requires more than an allegation that a defendant profited from a plaintiff’s personal identification information. Rather, **a plaintiff must allege how the defendant’s use of the information deprived the plaintiff of the information’s economic value.** ...Plaintiffs’ allegations certainly plead that Google made money using information about them for which they were provided no compensation beyond free access to Google’s services. But an allegation that Google profited is **not enough equivalent** to an allegation that such profiteering deprived Plaintiffs’ of economic value from that same information.”

23

---

---

---

---

---

---

---

---

## In re Google, Inc.

- “Plaintiffs still cite no case law holding that a **contract breach** by itself constitutes an **injury in fact.**”

24

---

---

---

---

---

---

---

---

## In re Google, Inc.

- What could be a sufficient injury?
  - Unauthorized use of system resources
  - Purchase of a new phone
  - Overpayment

25

---

---

---

---

---

---

---

---

## Data Breach Injury

- “In data breach cases, **most courts have rejected claims that the breach increased the risk of future identity theft**. See, e.g., *Amburgy v. Express Scripts, Inc.*, 671 F.Supp.2d 1046 (E.D. Mo. 2009); *Key v. DSW, Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006). Likewise, courts reject cases when plaintiffs spend money for mitigation expenses — measures to protect themselves against future harm.”

26

---

---

---

---

---

---

---

---

## B. TORT LAW

27

---

---

---

---

---

---

---

---

## Dwyer v. American Express Co.

- Issue
  - Is Amex liable for invasion of privacy and consumer fraud for its practice of renting information regarding cardholder spending habits?

28

---

---

---

---

---

---

---

---

## Dwyer v. American Express Co.

- "According to the news articles, defendants categorize and rank their cardholders into six tiers based on spending habits and then rent this information to participating merchants as part of a targeted joint-marketing and sales program. For example, a cardholder may be characterized as "Rodeo Drive Chic" or "Value Oriented." In order to characterize its cardholders, defendants analyze where they shop and how much they spend, and also consider behavioral characteristics and spending histories. Defendants then offer to create a list of cardholders who would most likely shop in a particular store and rent that list to the merchant."

29

---

---

---

---

---

---

---

---

## Dwyer v. American Express Co.

- What else?
  - Lists to target cardholders who purchase specific types of items
  - Joint-marketing ventures with merchants

30

---

---

---

---

---

---

---

---

## Dwyer v. American Express Co.

- Intrusion upon seclusion
  - "[There are] four elements [to **intrusion upon seclusion**] which must be alleged in order to state a cause of action: (1) an unauthorized intrusion or prying into the plaintiff's seclusion; (2) an intrusion which is offensive or objectionable to a reasonable man; (3) the matter upon which the intrusion occurs is private; and (4) the intrusion causes anguish and suffering..."

31

---

---

---

---

---

---

---

---

## Dwyer v. American Express Co.

- Why no unauthorized intrusion?
  - “By using the American Express card, a cardholder is **voluntarily**, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder’s spending habits and shopping preferences.”

32

---

---

---

---

---

---

---

---

## Dwyer v. American Express Co.

- “Defendants **rent names and addresses after they create a list of cardholders who have certain shopping tendencies**; they are not disclosing financial information about particular cardholders. These lists are being used **solely for the purpose of determining what type of advertising should be sent to whom**. We also note that the Illinois Vehicle Code authorizes the Secretary of State to sell lists of names and addresses of licensed drivers and registered motor-vehicle owners. Thus, **we hold that the alleged actions here do not constitute an unreasonable intrusion into the seclusion of another**. We so hold without expressing a view as to the appellate court conflict regarding the recognition of this cause of action.”

33

---

---

---

---

---

---

---

---

## Dwyer v. American Express Co.

- “[For] plaintiffs’ **appropriation claim**, the elements of the tort are: an appropriation, without consent, of one’s name or likeness for another’s use or benefit. This branch of the privacy doctrine is designed to protect a person from having his name or image used for commercial purposes without consent.”

34

---

---

---

---

---

---

---

---

## Dwyer v. American Express Co.

- “[P]laintiffs have **not stated a claim** for tortious appropriation because they have **failed to allege the first element**. Undeniably, each cardholder’s name is valuable to defendants. The more names included on a list, the more that list will be worth. However, **a single, random cardholder’s name has little or no intrinsic value** to defendants (or a merchant). Rather, an individual name has value only **when it is associated with one of defendants’ lists**. Defendants create value by categorizing and aggregating these names. Furthermore, defendants’ practices do not deprive any of the cardholders of any value their individual names may possess.”

35

---

---

---

---

---

---

---

---

## Selling Magazine Subscription Lists

- Court dismissed public disclosure tort action and appropriation tort action

36

---

---

---

---

---

---

---

---

## Sponsored Stories

- **“Sponsored Stories’ advertising program.** A Sponsored Story is a paid ad appearing on a person’s Facebook page. It **uses the name and photo** of a person’s friend who ‘likes’ the advertiser.”
- Plaintiff – advertising did not exist at the time the user signed up with Facebook and the use was sudden in ads

37

---

---

---

---

---

---

---

---

## Sponsored Stories

- Cause of action
  - appropriation of name or likeness under Cal. Civ. Code § 3344.
- Defense
  - Consent through terms of use

38

---

---

---

---

---

---

---

---

## Sponsored Stories

- “You can use your privacy settings to limit how your name and profile picture may be associated with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. You give us permission to use your name and [Facebook] profile picture in connection with that content, subject to the limits you place.”

39

---

---

---

---

---

---

---

---

## Sponsored Stories

- Plaintiffs alleged sufficient facts to establish injury to withstand a motion to dismiss
  - “Plaintiffs allege ... that they suffered economic injury because they were not compensated for Facebook’s commercial use of their names and likenesses in targeted advertisements to their Facebook Friends. ... [T]he Court finds nothing in the text of the statute or in case law that supports Defendant’s interpretation of § 3344 as requiring a plaintiff pleading economic injury to provide proof of preexisting commercial value and efforts to capitalize on such value in order to survive a motion to dismiss.”

40

---

---

---

---

---

---

---

---

## Private Investigators

- “The threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an **investigator has a duty to exercise reasonable care in disclosing a third person’s personal information to a client**. And we so hold. This is especially true when, as in this case, the investigator does not know the client or the client’s purpose in seeking the information.”
- Remsburg v. Docusearch, Inc. (N.H. 2003)

41

---

---

---

---

---

---

---

---

## Private Investigators

- “[A] person whose SSN is obtained by an investigator from a credit reporting agency without the person’s knowledge or permission **may have a cause of action for intrusion upon seclusion for damages caused by the sale of the SSN**, but must prove that the intrusion was such that it would have been offensive to a person of ordinary sensibilities.”

42

---

---

---

---

---

---

---

---

## Privacy Policy Violation = Intrusion on Seclusion?

- The basis for most of Plaintiffs’ claims is that Northwest’s website contained a privacy policy that stated that Northwest would not share customers’ information except as necessary to make customers’ travel arrangements. Plaintiffs contend that Northwest’s **provision of PNRs to NASA violated Northwest’s privacy policy**, giving rise to the legal claims noted above. ... the Court finds as a matter of law that the disclosure of Plaintiffs’ personal information would not be highly offensive to a reasonable person and that Plaintiffs have **failed to state a claim for intrusion upon seclusion.**”

43

---

---

---

---

---

---

---

---

## Deception under the FTC

- “A deceptive act or practice is a material ‘representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer’s detriment.’”

44

---

---

---

---

---

---

---

---

## Unfairness under the FTC

- “The FTC Act classifies a trade practice as unfair if it ‘causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition.’ 15 U.S.C. §45(n). Actions of a company can be both deceptive and unfair.”

45

---

---

---

---

---

---

---

---

## In the Matter of Snapchat, Inc.

- Issue
  - False or misleading regarding disappearance of snapchats

46

---

---

---

---

---

---

---

---



## In the Matter of Snapchat, Inc.

- “Snapchat provides a mobile application that allows consumers to send and receive photo and video messages known as ‘snaps.’ Before sending a snap, the application requires the sender to designate a period of time that the recipient will be allowed to view the snap. **Snapchat markets the application as an ‘ephemeral’ messaging application, having claimed that once the timer expires, the snap ‘disappears forever.’**”

47

---

---

---

---

---

---

---

---

## In the Matter of Snapchat, Inc.

- Are videos really gone?
  - Use of a computer and simple tools to locate and save the video
  - 3<sup>rd</sup> party applications to download and save videos and pics
  - Easy to circumvent screenshot notification detection mechanism

48

---

---

---

---

---

---

---

---

## In the Matter of Snapchat, Inc.

- “Snapchat has represented, expressly or by implication, that when sending a message through its application, the message will disappear forever after the user-set time period expires. [] In truth and in fact ... when sending a message through its application, the **message may not disappear forever** after the user-set time period expires. Therefore, the **representation ... is false or misleading.**”

49

---

---

---

---

---

---

---

---

## In the Matter of Snapchat, Inc.

- Result
  - 20 years of monitoring

50

---

---

---

---

---

---

---

---

## FTC Consent Decrees

- Elements include “(1) **prohibition on the activities** in violation of the FTC Act; (2) **steps to remediate** the problematic activities, such as software patches or notice to consumers; (3) **deletion** of wrongfully-obtained consumer data; (4) **modifications to privacy policies**; (5) **establishment of a comprehensive privacy program**, including risk assessment, appointment of a person to coordinate the program, and employee training, among other things; (6) **biennial assessment reports** by independent auditors; (7) **recordkeeping** to facilitate FTC enforcement of the order; (8) **obligation to alert** the FTC of any material changes in the company that might affect compliance obligations (such as mergers or bankruptcy filings).”

51

---

---

---

---

---

---

---

---

## Types of Section 5 Privacy and Security Violations

- “Deception” prong
  - “FTC brings cases for broken promises of privacy, general deception, insufficient notice, and unreasonable data security practices.”

52

---

---

---

---

---

---

---

---

## Types of Section 5 Privacy and Security Violations

- “Unfairness” prong
  - “[T]he FTC brings cases for retroactive changes to privacy policies, deceitful data collection, improper use of data, unfair design or unfair default settings, and unfair data security practices.”

53

---

---

---

---

---

---

---

---

## Retroactive Changes to Privacy Policies

- “Gateway **altered its privacy policy** to allow the renting of personal information to third parties **without informing customers and obtaining their explicit consent**. The FTC filed a complaint alleging that this practice was an unfair and deceptive act. According to the FTC, Gateway’s retroactive application of a **materially changed privacy policy** to information that it had previously collected constituted an unfair practice. The FTC also charged that Gateway’s **failure to inform consumers** of its changes to its privacy policies, despite its promises to do so, constituted a deceptive practice.”

54

---

---

---

---

---

---

---

---

## In the Matter of Facebook, Inc.

- Issue
  - Availability of certain posted information to unknown people

55

---

---

---

---

---

---

---

---

## In the Matter of Facebook, Inc.

- "Facebook has designed its Platform such that Platform Applications can **access user profile information** in two main instances. First, **Platform Applications that a user authorizes** can access the user's profile information. Second, if a **user's 'Friend' authorizes a Platform Application**, that application can **access certain [parts] of the user's profile information, even if the user has not authorized that Application**. For example, if a user authorizes a Platform Application that provides reminders about Friends' birthdays, that application could access, among other things, the birthdays of the user's Friends, even if these Friends never authorized the application."

56

---

---

---

---

---

---

---

---

---

---

## In the Matter of Facebook, Inc.

- "[Nothing on Facebook] disclosed that a **user's choice** to restrict profile information to 'only Friends' or 'Friends of Friends' **would be ineffective as to certain third parties**. Despite this fact, in many instances, Facebook has made profile information that a user chose to restrict to 'only Friends' or 'Friends of Friends' **accessible to any Platform Applications that the user's Friends have used** (hereinafter 'Friends' Apps'). Information shared with such Friends' Apps has included, among other things, a user's birthday, hometown, activities, interests, status updates, marital status, education (e.g., schools attended), place of employment, photos, and videos."

57

---

---

---

---

---

---

---

---

---

---

## In the Matter of Facebook, Inc.

- "[O]n approximately November 19, 2009, Facebook **changed its privacy policy** to designate certain user information as 'publicly available' ("PAI"). on approximately December 8, 2009, Facebook began implementing the changes referenced in its new policy ('the December Privacy Changes') to **make public in new ways** certain information that users previously had provided."

58

---

---

---

---

---

---

---

---

---

---

## In the Matter of Facebook, Inc.

- "Before December 8, 2009, users could, and did, use their Profile Privacy Settings to limit access to their Friend List. Following the December Privacy Changes, Facebook users could no longer restrict access to their Friend List through their Profile Privacy Settings, and **all prior user choices to do so were overridden**, making a user's Friend List **accessible to other users**. Although Facebook reinstated these settings shortly thereafter, they were not restored to the Profile Privacy Settings and instead were effectively hidden."

59

---

---

---

---

---

---

---

---

## In the Matter of Facebook, Inc.

- "Facebook failed to disclose, or failed to disclose adequately, that, following the December Privacy Changes, **users could no longer restrict access** to their Name, Profile Picture, Gender, Friend List, Pages, or Networks by using privacy settings previously available to them. Facebook also failed to disclose, or failed to disclose adequately, that the December Privacy Changes **overrode existing user privacy settings** that restricted access to a user's Name, Profile Picture, Gender, Friend List, Pages, or Networks. These facts would be material to consumers. Therefore, Facebook's failure to adequately disclose these facts, in light of the representation made, **constitutes a deceptive act or practice.**"

60

---

---

---

---

---

---

---

---

## In the Matter of Facebook, Inc.

- "[B]y designating certain user profile information publicly available that previously had been subject to privacy settings, **Facebook materially changed its promises that users could keep such information private**. Facebook **retroactively applied** these changes to personal information that it had previously collected from users, **without their informed consent**, in a manner that has caused or has been likely to cause substantial injury to consumers, was not outweighed by countervailing benefits to consumers or to competition, and was not reasonably avoidable by consumers. This practice **constitutes an unfair act or practice.**"

61

---

---

---

---

---

---

---

---

## In the Matter of Facebook, Inc.

- "Facebook has shared information about users with Platform Advertisers by **identifying to them the users who clicked on their ads** and to whom those ads were targeted. ... Facebook has represented, expressly or by implication, that Facebook does not provide advertisers with information about its users. ... Facebook has **provided advertisers with information about its users**. Therefore, the representation set forth ... constitutes a **false or misleading representation.**"

62

---

---

---

---

---

---

---

---

## In the Matter of Sears Holdings Management Corp.

- Issue
  - Did SHMC violate Section 5(a) of the Federal Trade Commission Act?
  - My SHC Community related app developed by a third party

63

---

---

---

---

---

---

---

---

## In the Matter of Sears Holdings Management Corp.

- "The Application, when installed, **runs in the background at all times** on consumers' computers and **transmits tracked information**, including nearly **all of the Internet behavior** that occurs on those computers, to servers maintained on behalf of respondent. Information collected and transmitted includes: web browsing, filling shopping baskets, transacting business during secure sessions, completing online application forms, checking online accounts, and, through select header information, use of web-based email and instant messaging services."

64

---

---

---

---

---

---

---

---

## In the Matter of Sears Holdings Management Corp.

- How was information communicated to users?
  - Pop up with information
  - Follow up email
  - Registration page with “Privacy Statement and User License Agreement”

65

---

---

---

---

---

---

---

---

## In the Matter of Sears Holdings Management Corp.

- “When installed, the **Application functioned and transmitted information substantially as described in the PSULA**. The Application, when installed, would run in the background at all times on consumers’ computers. Although the Application would be listed (as ‘mySHC Community’) in the ‘All Programs’ menu and ‘Add/Remove’ utilities of those computers, and the Application’s executable file name (‘srhc.exe’) would be listed as a running process in Windows Task Manager, the Application would display to users of those computers **no visible indication**, such as a desktop or system tray icon, **that it was running.**”

66

---

---

---

---

---

---

---

---

## In the Matter of Sears Holdings Management Corp.

- “The Application transmitted, in real time, tracked information to servers maintained on behalf of respondent. The tracked information included **not only information about websites consumers visited and links that they clicked**, but also the **text of secure pages**, such as online banking statements, video rental transactions, library borrowing histories, online drug prescription records, and select header fields that could show the sender, recipient, subject, and size of web-based email messages.”

67

---

---

---

---

---

---

---

---

## In the Matter of Sears Holdings Management Corp.

- “[R]espondent has represented, expressly or by implication, that the Application would **track consumers’ ‘online browsing’**” Respondent **failed to disclose** adequately that the software application, when installed, would: **monitor nearly all of the Internet behavior that occurs on consumers’ computers** ... to respondent’s remote computer servers. **These facts would be material to consumers in deciding to install the software. Respondent’s failure to disclose these facts, in light of the representations made, was, and is, a deceptive practice.**

68

---

---

---

---

---

---

---

---

## In the Matter of Sears Holdings Management Corp.

- “Respondent’s failure to disclose these [relevant] facts, in light of the representations made, was, and is, a deceptive practice.”

69

---

---

---

---

---

---

---

---

## Review of a Privacy Policy

- Select a privacy policy of a site
- What are your privacy expectations with the site before reviewing the privacy policy?
- How do you expect that the site makes money from your information (if at all)?
- How will your personal and non-personal information be used under the policy?
- How can your information be shared with third parties?
- Can your information be sold in any form?

70

---

---

---

---

---

---

---

---



## Terms of Use

71

---

---

---

---

---

---

---

---

## Terms of Use

- Are they enforceable?
- Why type of notice must be the user be put on to be enforceable?

72

---

---

---

---

---

---

---

---

## Terms of Use

- A web site should contain, in a prominent location, a hyperlink to the Terms and Conditions of Use, to which a user must agree in order to access or use the site. The provisions contained in the Terms and Conditions will vary depending on the type of web site, for example whether the site is "passive" or "active," whether the site accepts user submissions, and whether the site collects personal information from users.

73

---

---

---

---

---

---

---

---

**Specht v. Netscape  
Communications Corp**

- “[W]e are asked to determine whether [] plaintiffs [], by acting upon defendants’ invitation to download free software made available on defendants’ webpage, agreed to be bound by the software’s license terms (which included the arbitration clause at issue), even though plaintiffs could not have learned of the existence of those terms unless, prior to executing the download, they had scrolled down the webpage to a screen located below the download button.”

74

---

---

---

---

---

---

---

---

**Specht v. Netscape  
Communications Corp**

- Nature of underlying dispute - SmartDownload transmitted to defendants private information about plaintiffs’ downloading of files from the Internet

75

---

---

---

---

---

---

---

---

**Specht v. Netscape  
Communications Corp**

- “[Certain] plaintiffs acknowledge that when they proceeded to initiate installation of Communicator, they were automatically shown a scrollable text of that program’s license agreement and were not permitted to complete the installation until they had clicked on a ‘Yes’ button to indicate that they accepted all the license terms.”

76

---

---

---

---

---

---

---

---

**Specht v. Netscape  
Communications Corp**

- Plaintiffs expressly agreed to Communicator's license terms by clicking "Yes."
- If SmartDownload was downloaded, they were not provided with additional license terms
- "The sole reference to SmartDownload's license terms on the 'SmartDownload Communicator' webpage was located in text that would have become visible to plaintiffs only if they had scrolled down to the next screen."

77

---

---

---

---

---

---

---

---

**Specht v. Netscape  
Communications Corp**

- D.C. – plaintiff's are not subject to the license agreements because they were not provided with sufficient notice

78

---

---

---

---

---

---

---

---

**Specht v. Netscape  
Communications Corp**

- "[W]e conclude that the district court properly decided the question of reasonable notice and objective manifestation of assent as a matter of law on the record before it, and we decline defendants' request to remand for a full trial on that question."

79

---

---

---

---

---

---

---

---

**Specht v. Netscape  
Communications Corp**

- “Whether governed by the common law or by Article 2 of the Uniform Commercial Code (‘UCC’), a transaction, in order to be a contract, requires a manifestation of agreement between the parties.”
- “Arbitration agreements are no exception to the requirement of manifestation of assent.”

80

---

---

---

---

---

---

---

---

**Specht v. Netscape  
Communications Corp**

- “We disagree with the proposition that a reasonably prudent offeree in plaintiffs’ position would necessarily have known or learned of the existence of the SmartDownload license agreement prior to acting, so that plaintiffs may be held to have assented to that agreement with constructive notice of its terms.”

81

---

---

---

---

---

---

---

---

**Specht v. Netscape  
Communications Corp**

- “Plaintiffs were responding to an offer that did not carry an immediately visible notice of the existence of license terms or require unambiguous manifestation of assent to those terms.”
- “We conclude that in circumstances such as these, where consumers are urged to download free software at the immediate click of a button, a reference to the existence of license terms on a submerged screen is not sufficient to place consumers on inquiry or constructive notice of those terms.”

82

---

---

---

---

---

---

---

---

## Nguyen v. Barnes & Noble Inc.

- Barnes & Noble appeal of DC denial to compel arbitration against Nguyen pursuant to the arbitration agreement contained in its website's Terms of Use

83

---

---

---

---

---

---

---

---

## Nguyen v. Barnes & Noble Inc.

- Nature of dispute
  - Nguyen purchases 2 touchpads and the orders are cancelled by Barnes & Noble the next day
  - Class action lawsuit

84

---

---

---

---

---

---

---

---

## Nguyen v. Barnes & Noble Inc.

- "The website's Terms of Use are available via a 'Terms of Use' hyperlink located in the bottom left-hand corner of every page on the Barnes & Noble website, which appears alongside other hyperlinks labeled 'NOOK Store Terms,' 'Copyright,' and 'Privacy Policy.' These hyperlinks also appear underlined and set in green typeface in the lower lefthand corner of every page in the online checkout process."

85

---

---

---

---

---

---

---

---

### Nguyen v. Barnes & Noble Inc.

- “Nguyen neither clicked on the ‘Terms of Use’ hyperlink nor actually read the Terms of Use. Had he clicked on the hyperlink, he would have been taken to a page containing the full text of Barnes & Noble’s Terms of Use.”
- “Nguyen contends that he cannot be bound to the arbitration provision because he neither had notice of nor assented to the website’s Terms of Use.”

86

---

---

---

---

---

---

---

---

### Nguyen v. Barnes & Noble Inc.

- “Because no affirmative action is required by the website user to agree to the terms of a contract other than his or her use of the website, the determination of the validity of the browsewrap contract depends on whether the user has actual or constructive knowledge of a website’s terms and conditions.”

87

---

---

---

---

---

---

---

---

### Nguyen v. Barnes & Noble Inc.

- “[C]ourts have consistently enforced browsewrap agreements where the user had actual notice of the agreement.”
- “Courts have also been more willing to find the requisite notice for constructive assent where the browsewrap agreement resembles a clickwrap agreement—that is, where the user is required to affirmatively acknowledge the agreement before proceeding with use of the website.”

88

---

---

---

---

---

---

---

---

## Nguyen v. Barnes & Noble Inc.

- “But where, as here, there is no evidence that the website user had actual knowledge of the agreement, the validity of the browsewrap agreement turns on whether the website puts a reasonably prudent user on inquiry notice of the terms of the contract. ... Whether a user has inquiry notice of a browsewrap agreement, in turn, depends on the design and content of the website and the agreement’s webpage. ... Where the link to a website’s terms of use is buried at the bottom of the page or tucked away in obscure corners of the website where users are unlikely to see it, courts have refused to enforce the browsewrap agreement.”

89

---

---

---

---

---

---

---

---

## Nguyen v. Barnes & Noble Inc.

- “[W]e therefore hold that where a website makes its terms of use available via a conspicuous hyperlink on every page of the website but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent, even close proximity of the hyperlink to relevant buttons users must click on—without more—is insufficient to give rise to constructive notice.”

90

---

---

---

---

---

---

---

---

## Nguyen v. Barnes & Noble Inc.

- “[W]e hold that Nguyen did not enter into Barnes & Noble’s agreement to arbitrate.”

91

---

---

---

---

---

---

---

---

## Manifestation of Assent

- What could BN have done?
  - Check box accepting terms before proceeding with login
  - Further notice before checkout
  - Better font contrast

92

---

---

---

---

---

---

---

---

***Program  
Completed***

© 2015-2016 Randy L. Canis

93

---

---

---

---

---

---

---

---