Santa Clara University

Online Marketing Law Updates

Prof. Eric Goldman

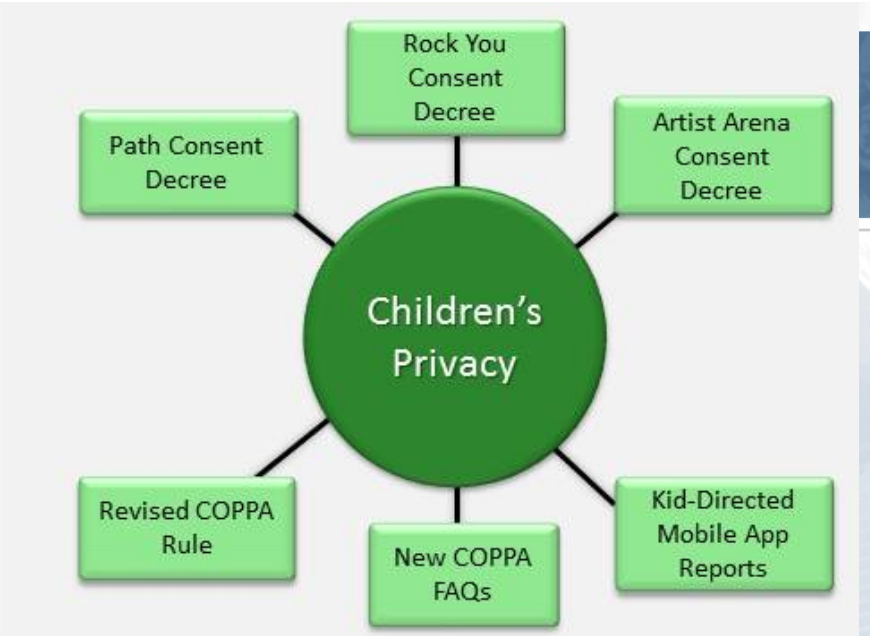
Director, High Tech Law Institute

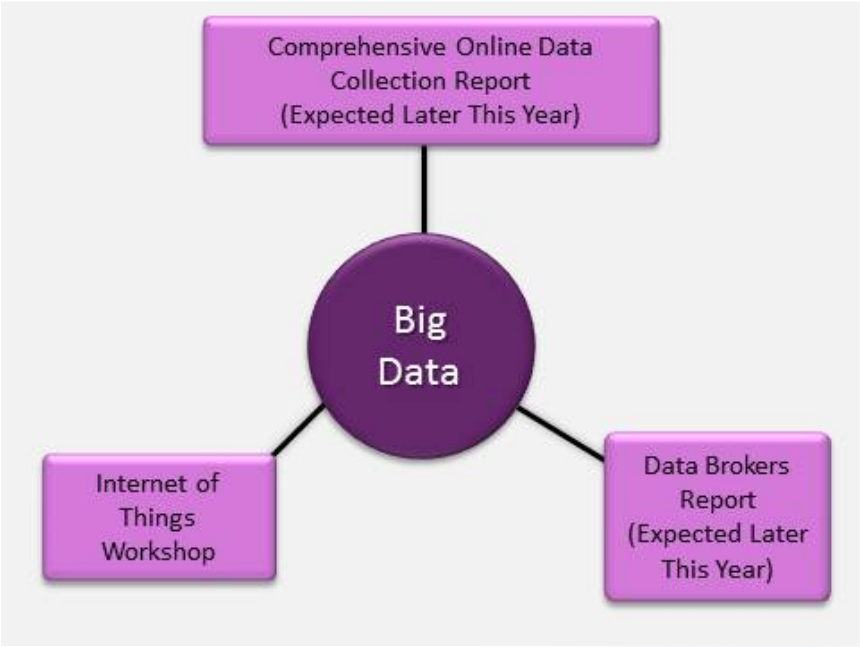
http://www.ericgoldman.org • http://hightechlaw.scu.edu

egoldman@gmail.com

Santa Clara University

The Jesuit university in Silicon Valley





- http://www.insideprivacy.com/united-states/federal-trade-commission/ftcs-enforcement-priorities-infographic/, attributed to Assistant Director Chris Olsen and Senior Attorney Peder Magee, both of the Federal Trade Commission's Division of Privacy and Identity Protection

Santa Clara University

COPPA

- Applies to website/online service that “targets” kids or has “actual knowledge” it’s collecting data from kids
- Upcoming changes
  - Extend COPPA to apps
  - Extend COPPA to ad networks
  - Expansion of “personal information”
- Avoidance strategies
  - Non-kids sites
    - Don’t collect age or related info (grade level)
    - If collect age info, bounce kids, delete their info, place blocking cookie
  - Kids sites
    - NO LONGER WORKS: avoid collecting “personal information”
    - Age-authenticate visitors immediately upon arrival (safe harbor)

Santa Clara University

FTC as Security Breach Enforcer

- Wyndham Hotels' allegedly deficient security measures
  - No firewalls
  - Passwords stored in clear text
  - Connected "insecure" servers to network running outdated software with known vulnerabilities and using vendor-supplied default passwords
  - Didn't require complex passwords
  - Didn't inventory devices on the network
  - Didn't take reasonable steps to find/prevent intrusions, and didn't properly remediate intrusions
  - Failed to adequately restrict vendor access to network
- Result: hackers obtained personal data 3x over 2 years and allegedly generated $10.6M of losses

Santa Clara University

FTC as Security Breach Enforcer

- FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce"
  - "Since 2000, the FTC has brought more than forty data security cases, nineteen of which alleged unfair practices."
  - "The FTC is not suing Wyndham for the fact that it was hacked, it is suing Wyndham for mishandling consumers' information such that hackers were able to steal it."

. . . We recognize the importance of protecting the privacy of individual-specific (personally identifiable) information collected about guests, callers to our central reservation centers, visitors to our Web sites, and members participating in our Loyalty Programs (collectively 'Customers'). . . .

This policy applies to residents of the United States, hotels of our Brands located in the United States, and Loyalty Program activities in the United States only. . . .

We safeguard our Customers' personally identifiable information by using industry standard practices. Although "guaranteed security" does not exist either on or off the Internet, we make commercially reasonable efforts to make our collection of such Information consistent with all applicable laws and regulations. Currently, our Web sites utilize a variety of different security measures designed to protect personally identifiable information from unauthorized access by users both inside and outside of our company, including the use of 128-bit encryption based on a Class 3 Digital Certificate issued by Verisign Inc. This allows for utilization of Secure Sockets Layer, which is a method for encrypting data. This protects confidential information – such as credit card numbers, online forms, and financial data – from loss, misuse, interception and hacking. We take commercially reasonable efforts to create and maintain "fire walls" and other appropriate safeguards to ensure that to the extent we control the Information, the Information is used only as authorized by us and consistent

FTC as Security Breach Enforcer

New best practice: no puffery in privacy policies—JUST THE FACTS

Santa Clara University

Privacy Hot Spots at Agencies

- Blogger/Social Media Promotions
  - Advertiser best practices
    - Require disclosure in blog posts
    - Monitor bloggers for compliance
  - No action: Nordstrom, Hyundai, Ann Taylor LOFT
  - Action: Legacy Learning (fake affiliate reviews)
- CA's Privacy Enforcement and Protection Unit
  - B&P 22575-79: websites must display privacy policy
  - App stores will enforce rule
  - People v. Delta Airlines: dismissed due to Airline Deregulation Act

Santa Clara University

More Privacy Hot Spots

- Privacy class action lawsuits
  - Standing
  - “Lost money or property”/substantive harms
  - Cy pres
- Do-Not-Track
- Mobile Marketing: No clearly legal way to do text message marketing
- Social Media account ownership
  - Group A: Independent parties battling over username/account
  - Group B: Co-venturers/employees
  - State employee privacy statutes (e.g., CA AB 1844)

Santa Clara University

Recap

Have privacy policies gotten so regulated that only specialists should draft them?

Santa Clara University

Keyword Advertising

- Lawsuits against Google are losers
  - Won or settled all but 2 TM cases (Parts.com and Ison)
  - Won in Australia
  - Liberalized its policy globally
- Competitive lawsuits are losers
  - Plaintiff TM win rate: 4 of 14 (none since 2011)
    - Plaintiffs haven't won a jury trial
    - General Steel v. Chumley: insufficient confusion when advertiser uses TM in ad copy in non-comparative way
    - No publicity rights workaround (Habush v. Cannon)
  - ECONOMICALLY IRRATIONAL
    - Storus v. Aroa: 1,374 clicks over 11 months
    - King v. ZymoGenetics: 84 clicks
    - Sellify v. Amazon: 1,000 impressions and 61 clicks
    - 800-JR Cigar v. GoTo.com: $345 in revenue
    - 1-800 Contacts v. Lens.com: $20 of profit
    - InternetShopsInc.com v. Six C: 1,319 impressions, 35 clicks, no sales

Santa Clara University