CENTER FOR JUSTICE & DEMOCRACY
185 WEST BROADWAY
NEW YORK, NY 10013
TEL: 212.431.2882
centerjd@centerjd.org
http://centerjd.org

FAQ: PRIVACY AND FORCED ARBITRATION – WHY IT MATTERS

How might companies violate your privacy?

Companies have more ways than ever to violate privacy rights. Explains the Electronic Frontier Foundation, "New technologies are radically advancing our freedoms but they are enabling unparalleled invasions of privacy."[1] For example, as one blogger put it, "[B]ecause most modern tech companies provide free services and depend nearly entirely on advertising revenue, their interests in data mining for targeted advertising will always run counter to users' privacy rights."[2] Through social media platforms and other communication tools, technology companies can easily share private messages or search histories, harvest biometric data about users or sell personal information, like geolocation records, to the highest-bidding third party. Advertisers might use a person's name and picture to promote online products without permission.

In addition, healthcare providers can release information about a person's private illness history, treatments and medications without the patient's consent. Stores may fail to prevent in-store security breaches, just as banks and lenders can fail to prevent data breaches. Hotels and employers might even secretly record private conversations without the knowledge or consent of the party whose privacy is being breached, in violation of the law.

What kinds of harms might result from invasions of privacy?

Privacy invasions can have severe consequences for a person's professional and personal life. Incorrect, misleading or embarrassing information may hurt someone's employment potential, making that individual less likely to be hired or more likely to be fired. Privacy violations can destroy important personal relationships, damage someone's standing in child custody or other legal proceedings or create a hurtful stigma that follows for a lifetime. Illegally or illegitimately released personal information can also be used to discriminate. It might result in increased costs for insurance, products or services. It can even lead to issues of safety or physical harm if the information is used to stalk or inform criminals of security vulnerabilities.

Identity theft is another possible harm. Thieves might gain access to someone's name, address, credit and banking information, social security number, medical insurance or biometric data.[3] With this information criminals can wreak havoc on someone's life, emptying their bank account,[4] ruining their credit, obtaining medical care under their name and even pretending to be

them if ever arrested.[5] Repairing such damage can take years and cost thousands of dollars, not to mention take a significant psychological and emotional toll on victims and their families.

What kinds of laws protect a person's privacy?

Many state and federal laws exist to protect the privacy of individuals. Federal laws that regulate how, when and why a consumer's data may be intercepted, stored or used include: the Fair Credit Reporting Act[6]; the Driver's Privacy Protection Act[7]; the Health Insurance Portability and Accountability Act (HIPPA)[8]; the Electronic Communications Privacy Act[9]; the Stored Communications Act[10]; and the Children's Online Privacy Protection Act.[11] In addition, some states have laws to protect insurance and library records, student and credit information, tracking technologies and more. For example, California's Invasion of Privacy Act[12] bars eavesdropping on private communications and Pennsylvania's Wiretapping and Electronic Surveillance Control Act[13] prohibits unauthorized access to computer networks, files and systems.

Are these laws enough to ensure that someone's privacy is protected?

No, laws alone are not enough. Government agencies are too overworked and under-resourced to effectively monitor and enforce privacy law violations. For example, as a joint ProPublica/*Wired* article explained, "The FTC is the lead agency in the government's effort to ensure that companies do not cross the still-hazy border between acceptable and unacceptable data collection. But the agency's ambitions are clipped by a lack of both funding and legal authority," with the FTC "ill-equipped to find out, on its own, what companies like Google and Facebook are doing behind the scenes."[14] In fact, until very recently, the agency only employed a small handful of privacy technologists.[15]

Can private litigation help enforce privacy laws and vindicate rights?

Yes. Many state and federal privacy laws allow individuals or groups of individuals (classes) to file lawsuits in order to protect their rights. Through litigation consumers can force a company to stop illegal behavior, obtain compensation for the harms they have suffered and compel public disclosure about privacy violations.

In the past few years, corporations such as LinkedIn, Six Continents Hotels and many others have been taken to court by consumers – not regulators – to enforce state and federal privacy laws.[16] For example, in 2013, students and teachers sued Google for allegedly scanning the contents of student Gmail accounts, gathering information and creating personal student profiles that could be used for targeted advertising in violation of state and federal privacy laws, including the Electronic Communications Privacy Act, California's Invasion of Privacy Act and Maryland's Wiretap Act.[17] Google settled the case. It also agreed to stop reading and mining students' email for advertising purposes.[18]

Many privacy cases have been brought as class actions.[19] In 2010, Countrywide Financial, Countrywide Home Loans and Bank of America settled with a class of customers for stealing thousands, perhaps millions, of customers' private financial information to sell to third parties. After learning of the breach, Countrywide waited months to inform customers – exposing them to a high risk of identity theft and ruined credit histories – which made it impossible for plaintiffs to secure legitimate loans and lines of credit. As part of the settlement, class members were eligible to receive up to $50,000 per incident up to a total of $5 million.[20] In 2007, Bank of America settled with a class of customers for disclosing personal information to third party marketers without consent or notice in exchange for money.[21] In 2006, Fidelity Federal Bank settled with a class of 565,000 customers for obtaining driver registration information, which it used for marketing, in alleged violation of the Driver's Privacy Protection Act. Fidelity agreed to pay $50 million and destroy any personal information of class members that was illegally obtained from motor vehicle records.[22]

What are forced arbitration clauses and class action waivers, and how do they impact consumers' ability to seek justice for privacy violations?

Forced arbitration clauses – hidden in the fine print of most consumer contracts today and written in legalese that is incomprehensible to most people – prohibit harmed individuals from suing law-breaking companies in court. Instead, they must resolve their disputes in secretive, corporate- controlled, rigged arbitration systems. These clauses also typically prevent consumers from joining together with other victims in class action lawsuits.

Companies have used forced arbitration clauses and class action bans to avoid accountability for violations of customer privacy. Take social media providers, who, according to a 2014 study, frequently require customers to submit to arbitration in their "terms of use" agreements as a condition of using their services, essentially constructing a "liability-free zone" where consumers have "rights without remedies" if the companies invade their privacy.[23] This is especially problematic given that such providers include dating, professional networking, photo sharing, apartment finding and communications websites, who possess an incalculable amount of sensitive consumer data.[24]

What is wrong with forced arbitration?

Consumers are extremely disadvantaged in arbitration controlled by companies. Arbitrators are often in contract with the businesses against which a claim is brought. Arbitration companies have a financial incentive to side with corporate repeat players who generate most of the cases they handle. Arbitrators are also not required to have any legal training and they need not follow the law. Court rules of evidence and procedure that exist to protect consumers do not apply. Arbitration proceedings are secretive. Decisions are enforceable with the full weight of the law even though they may be legally incorrect. This is extremely disturbing because such decisions are binding. Sometimes, victims must split the sizeable costs of arbitration with the defense. But even if the defense handles the costs, this gives them the ability to "freeze" a proceeding in the rare situation where it seems the arbitrator is moving against them.[25]

Why should victims of privacy violations have access to the courts?

With money and politics already dominating the executive and legislative branches of government, America's court system is one of the only places left in America where everyday people can successfully confront powerful industries and institutions. Indeed, the right of harmed or violated people to vindicate their rights in court is a fundamental precept of American democracy. More specifically, class actions, which allow people to band together in a lawsuit, are one of the most important tools of justice for victims of privacy violations. Where a company may have acquired a large financial windfall by violating the privacy of large numbers of people, class actions are often the only way for victims to hold the company accountable. Victims then have the option of seeking compensation as well as the ability to ask a court to stop the violations.[26] They also have the right to appeal an unfair initial decision.[27] Forced arbitration eliminates these options.

NOTES

[1] Electronic Frontier Foundation, "Privacy," https://www.eff.org/issues/privacy (viewed April 22, 2016).
[2] William Peacock, "Next Big Practice Area: Privacy Class Action Lawsuits?" *Technologist*, January 6, 2014, http://blogs.findlaw.com/technologist/2014/01/next-big-practice-area-privacy-class-action-lawsuits.html
[3] Federal Trade Commission, "Avoiding Identity Theft," https://www.consumer.gov/articles/1015-avoiding-identity-theft (viewed April 22, 2016); Marc Goodman, "You Can't Replace Your Fingerprints," *Slate Magazine*, February 24, 2015, http://www.slate.com/articles/technology/future_tense/2015/02/future_crimes_excerpt_how_hackers_can_steal_fingerprints_and_more.html
[4] *See*, *e.g.*, Kevin Rowson, "Identity thief drained family's savings," *WXIA-TV* (*Atlanta 11 Alive News*), April 8, 2016, http://www.11alive.com/money/identity-thief-drained-familys-savings/125112071
[5] Federal Trade Commission, "Avoiding Identity Theft," https://www.consumer.gov/articles/1015-avoiding-identity-theft (viewed April 22, 2016).
[6] Federal Trade Commission, "A Summary of Your Rights Under the Fair Credit Reporting Act." https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf (viewed April 22, 2016).
[7] Electronic Privacy Information Center, "The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record," https://epic.org/privacy/drivers/ (viewed April 22, 2016).
[8] U.S. Department of Health and Human Services, "Health Information Privacy," http://www.hhs.gov/hipaa/ (viewed April 22, 2016).
[9] U.S. Department of Justice, "Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22," https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last revised July 30, 2013).
[10] 18 U.S.C. § 2701, https://www.law.cornell.edu/uscode/text/18/2701
[11] 15 U.S.C. §§ 6501–6505, https://www.law.cornell.edu/uscode/text/15/chapter-91
[12] Cal. Penal Code §§ 630 et seq., http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=630-638.53
[13] 18 Pa. C.S.A. §§5701 et seq., http://www.legis.state.pa.us/cfdocs/legis/LI/consCheck.cfm?txtType=HTM&ttl=18&div=0&chpt=57
[14] Peter Maass, "Your FTC Privacy Watchdog: Low-Tech, Defensive, Toothless," *ProPublica*/*Wired*, June 28, 2012, http://www.wired.com/2012/06/ftc-fail/
[15] Ibid.
[16] For example, LinkedIn users filed a class action claiming violations of the California Invasion of Privacy Act, the Stored Communications Act and the federal Wiretap Act, among other laws, after the company allegedly sent multiple reminder emails on members' behalf without their consent. Under the settlement, LinkedIn agreed to revise its disclosures and implement new functionality that allowed members to control whether reminder emails were sent. *Perkins v. LinkedIn Corporation*, Case No. 13-cv-04303-HRL (N.D. Cal.)(notice of class action and

proposed settlement)(September 15, 2015), http://www.addconnectionssettlement.com/media/381770/v7_lnkd1_notice_092815_final.pdf. Similarly, it took a consumer class action for Six Continents Hotels -- owner of Holiday Inn Express, Crowne Plaza Hotels and Resorts, InterContinental Hotels and Resorts, among other hotel chains -- to compensate thousands of customers after allegedly monitoring and recording customer-initiated phone calls, which often contained sensitive personal information, without customer consent in violation of California's Invasion of Privacy Act. Maya Rajamani, "Hotel Co. Pays $11.7M To Settle Recorded Calls Suit," *Law360,* http://www.law360.com/articles/674528/hotel-co-pays-11-7m-to-settle-recorded-calls-suit, discussing *McCabe v. Six Continents Hotel,* Case No. 12-cv-04818 NC (N.D. Cal.)(order granting class certification and preliminary approval of class action settlement)(June 30, 2015), https://www.hotelcallrecordingsettlement.com/documenthandler.ashx?docpath=/documents/preliminary_approval_order.pdf.

[17] Benjamin Herold, "Google Under Fire for Data-Mining Student Email Messages," *Education Week*, March 13, 2014, http://www.edweek.org/ew/articles/2014/03/13/26google.h33.html, discussing *In Re Google Inc. Gmail Litigation*, Master Docket No. 5:13-md-02430-LHK (N.D. Cal.)(plaintiffs' consolidated individual and class action complaint)(filed May 16, 2013), http://www.consumerwatchdog.org/resources/gmailcomplaint051613.pdf

[18] Alistair Barr, "Google Stops Scanning Student Gmail Accounts for Ads," *Wall Street Journal Digits Blog*, April 30, 2014, http://blogs.wsj.com/digits/2014/04/30/google-stops-scanning-student-gmail-accounts-for-ads/; Lauren Williams, "Under Pressure Of Lawsuits, Google Says It Will Stop Reading Students' Emails (Updated)," *ThinkProgress*, April 30, 2014, http://thinkprogress.org/justice/2014/04/30/3432582/google-scans-students-gmail/

[19] See, e.g., *In re Carrier IQ, Inc. Consumer Privacy Litigation*, http://topclassactions.com/lawsuit-settlements/lawsuit-news/329419-9m-tabletsmartphone-privacy-class-action-settlement-preliminarily-approved/, http://www.prnewswire.com/news-releases/hagens-berman-sobol-shapiro-llp-and-pearson-simon--warshaw-llp-announce-proposed-settlement-of-carrier-iq-inc-consumer-privacy-litigation-300246708.html; Health Net data breach, http://www.databreachtoday.com/health-net-breach-lawsuit-settled-a-7099, http://www.girardgibbs.com/media/files/93_healthnet-class-notice.pdf*; Blue Cross of California Website Security Cases,* http://www.prnewswire.com/news-releases/class-settlement-preliminarily-approved-in-blue-cross-of-california-website-security-cases-case-no-jccp-4647-pending-in-orange-county-superior-court-125746573.html, http://www.amednews.com/article/20110801/business/308019961/7/

[20] Sarah Pierce, "Countrywide Settles Data Theft Class Action Lawsuit," *Top Class Actions,* May 4, 2010, http://www.topclassactions.com/lawsuit-settlements/lawsuit-news/632-countrywide-settles-data-theft-class-action-lawsuit/; Sarah Pierce, "Countrywide Sued for 'Aiding and Abetting' Customer Identity Theft," *Top Class Actions*, April 7, 2010, http://www.topclassactions.com/lawsuit-settlements/lawsuit-news/585-countrywide-sued-for-aiding-and-abetting-customer-identity-theft/; *In Re: Countrywide Financial Corp. Customer Security Breach Litigation*, No. 3:08-md-01998-TBR, MDL 1998 (W.D. Ky.), http://www.kywd.uscourts.gov/multidistrict-litigation/mdl-1998

[21] *Utility Consumers' Action Network v. Bank of America N.A.,* No. CJC-01-004211(Super. Ct. Cal.)(final settlement agreement)(2007), http://www.bankprivacycase.com/Documents/Final%20Settlement%20Agreement.pdf

[22] *Kehoe v. Fidelity Federal Bank and Trust*, (2006), No. 03-80593-CIV (S.D. Fla.)(settlement agreement and release)(July 21, 2006), http://www.sec.gov/Archives/edgar/data/1028336/000119312506163732/dex101.htm

[23] Thomas H. Koenig and Michael L. Rustad, "Fundamentally Unfair: An Empirical Analysis of Social Media Arbitration Clauses," p.341, 65Cas. W.Res. L. Rev.341 (2014). http://scholarlycommons.law.case.edu/caselrev/vol65/iss2/5/

[24] Ibid.

[25] *See, e.g.*, "Public Justice Comments to Bureau of Consumer Financial Protection In Response to Request for Information for Study of Pre-Dispute Arbitration Agreements," Docket No. CFPB-2012-0017, June 23, 2012, http://publicjustice.net/sites/default/files/downloads/PublicJusticeCommentsToCFPB_ReMandatoryArbitration_Jun2012.pdf

[26] Paul Bland, "Cheated Again: New Forced-Arbitration Decision Wipes Away Crucial California Consumer Protection Law," *Public Justice Blog*, October 29, 2013, https://www.publicjustice.net/cheated-again-new-forced-arbitration-decision-wipes-away-crucial-california-consumer-protection-law/, discussing *Ferguson v. Corinthian Colleges*, 733 F.3d 928 (9th Cir. 2013), http://cdn.ca9.uscourts.gov/datastore/opinions/2013/10/28/11-56965.pdf

[27] Thomas H. Koenig and Michael L. Rustad, "Fundamentally Unfair: An Empirical Analysis of Social Media Arbitration Clauses," 65 *Case W. Res. L. Rev.* 341, 343 (2014), http://scholarlycommons.law.case.edu/caselrev/vol65/iss2/5