2014

The FTC and Privacy and Security Duties for the Cloud

Daniel J. Solove

The FTC and Privacy and Security Duties for the Cloud

Daniel J. Solove & Woodrow Hartzog

2014

13 BNA Privacy & Security Law Report 577

Electronic copy available at: https://ssrn.com/abstract=2424998

Bloomberg BNA

Privacy and Security Law Report®

The FTC and Privacy and Security Duties for the Cloud

BY DANIEL J. SOLOVE AND WOODROW HARTZOG

Third-party data service providers, especially providers of cloud computing services, present unique and difficult privacy and data security challenges. While many companies that directly collect data from consumers are bound by the promises they make to individuals in their privacy policies, cloud service providers are usually not a part of this arrangement. It is not entirely clear what, if any, obligations cloud service providers have to protect the data of individuals with whom they have no contractual relationship. This problem is especially acute because many institutions sharing personal data with cloud service providers fail to include significant privacy and security protections in the contracts that govern the exchanges. Individuals can thus be placed at the mercy of contracts that they did not negotiate and that offer insufficient protection of their data.

Daniel J. Solove is the John Marshall Harlan research professor of law at George Washington University Law School and the chief executive officer of TeachPrivacy, http://teachprivacy.com, a privacy and data security training company.

Woodrow Hartzog is an assistant professor at Samford University's Cumberland School of Law and an affiliate scholar at the Center for Internet and Society at Stanford Law School.

The authors would like to thank Safegov.org for its support. All views in this piece are those of the authors and are not those of any organization with which they are affiliated.

For example, a study conducted by Fordham School of Law's Center on Law and Information Policy revealed that contracts between K-12 school districts and cloud service providers lacked essential terms for the protection of student data.[1] Many of the agreements analyzed failed to give the school districts the right to audit and inspect the vendor's practices with respect to the transferred data.[2] The agreements also failed to prohibit or limit redisclosure of student data or other confidential information.[3] No agreement "specifically prohibited the sale and marketing of children's information."[4]

In situations like the one above, students are caught in the crossfire, because their interests are often ignored in these contracts unless the schools fight for them, and it appears from the study that many schools lack the knowledge, expertise and resources to establish the appropriate contractual arrangements. In the context of schools, the Department of Education (DOE) under the Family Educational Rights and Privacy Act (FERPA) has very little ability to do much about it. Unlike the Department of Health and Human Services, which can enforce the Health Insurance Portability and Accountability Act directly against most entities that receive protected health information, the DOE has no direct authority under FERPA to regulate companies receiving education records.[5]

---

[1] Joel Reidenberg et al., *Privacy and Cloud Computing in Public Schools*, in Ctr. on Law and Info. Policy Book 2 (2013), *available at* http://ir.lawnet.fordham.edu/clip/2/; *see also* Daniel Solove, *Why Schools Are Flunking Privacy and How They Can Improve*, LinkedIn (Dec. 17, 2013), http://www.linkedin.com/today/post/article/20131217054543-2259773-why-schools-are-flunking-privacy-and-how-they-can-improve.

[2] Reidenberg, *supra* note 1, at 25.

[3] *Id.* at 28.

[4] *Id.*

[5] *See* Bryan Thurmond, *Dismantling a Dual-Headed System of Governance: How a Regulatory Overlap Undercuts the Security of Student Health Information in Public Schools*, 64 Admin L. Rev. 701, 707 (2012) ("[A]s spending legislation, [the DOE] enforces FERPA's provisions through the disbursement or rescission of federal education funds."); Benjamin F. Sidbury, *Gonzaga University v. Doe and Its Implications: No Right to Enforce Student Privacy Rights Under FERPA*, 29 J.C. & U.L. 655, 657 (2003) (footnote omitted) (citations omitted) ("[T]he language of [20 U.S.C. § 1232g(b)(1)] suggests that FERPA does not impose a per se prohibition on the disclosure

 ISSN 1538-3423

Situations such as the one above can also emerge whenever any organization enlists the assistance of a cloud service provider. Consumer data are shared with the cloud service provider, and consumers have no direct relationship with that provider. It is up to the organization to establish the appropriate relationship with cloud service providers. Some organizations do so quite well, but others can fall short.

Under these circumstances, what protects individuals whose personal data are shared by an organization with a third party? An emerging body of Federal Trade Commission (FTC) enforcement actions suggests that there can be a potentially robust set of protections—even in contexts that have thus far fallen outside of FTC jurisdiction, such as student data maintained by schools. In particular, we note that there are two emerging strands of FTC jurisprudence that can address these issues. The first pertains to data stewardship for the organizations that share personal data with cloud service providers. And the second pertains to third-party beneficiaries, where the FTC has recognized that consumers need not be a primary party to a contract in order to receive protection under the FTC Act. These two strands are essentially flip sides of the same coin. Under this approach, data collectors must act as data stewards and protect consumers when the organization shares information with a cloud provider. Likewise, the cloud service provider also owes a duty to consumers, who are essentially third-party beneficiaries of the data collector's efforts to ensure privacy and data security in their institutional bargaining.

Standards of Data Stewardship

Since the 1990s, the FTC has been regulating companies in privacy and security matters under Section 5 of the FTC Act. This statute prohibits ''unfair or deceptive acts or practices in or affecting commerce.''[6] The FTC has brought an extensive number of cases for problematic privacy and data security practices. We discuss in more detail how the FTC has gone about crafting a law of privacy from the ground up in our forthcoming article, ''The FTC and the New Common Law of Privacy.''[7] Privacy and data protection attorneys at the large law firms, in-house counsel and attorneys everywhere else follow the FTC closely. They look to the FTC for guidance about standards to follow. Thus far, the FTC has been more of a standard codifier than a standard maker. Instead of blazing a trail by creating new norms and standards, the FTC has waited until norms and standards have developed and then begun enforcement.

Once the FTC has enforced based on a particular standard, that standard achieves a new level of legitimacy and formality. For all intents and purposes, the standard becomes law. Because the law of privacy and data security is so fragmented, so magma-like in its nature, the FTC has had an unusually influential role in shaping the law of privacy and data security by embracing certain standards and norms that have achieved a decent level of consensus. For a long time, these standards have focused on what companies must do to protect the privacy and data security of personal data that they maintain. This year, however, an FTC case focuses on the standards for how a company shares personal data with external data service providers.

The case, *In re GMR Transcription Services Inc.*, involved the inadvertent exposure of people's medical data maintained by GMR, a company that provides medical transcription services.[8] The FTC concluded that GMR's failure to adequately choose, contract with and oversee a data service provider constituted an unfair and deceptive trade practice.[9]

According to the FTC complaint, GMR failed to ''adequately verify that their service provider, Fedtrans, implemented reasonable and appropriate security measures to protect personal information in audio and transcript files on Fedtrans' network and computers used by Fedtrans' typists.''[10] Moreover, the FTC faulted GMR for failures in contracting with its data service provider. The FTC complaint alleged that GMR failed to:

> (1) require Fedtrans by contract to adopt and implement appropriate security measures to protect personal information in medical audio and transcript files, such as by requiring that files be securely stored and securely transmitted to typists (e.g., through encryption) and authenticating typists (e.g., through unique user credentials) before granting them access to such files; and
>
> (2) take adequate measures to monitor and assess whether Fedtrans employed measures to appropriately protect personal information under the circumstances. . . .[11]

The FTC additionally found GMR to be deficient in doing due diligence before hiring its data service provider.[12] Looking broadly at the complaint, there are three key things that the FTC is now requiring companies to do when it comes to contracting with data service providers: (1) exercise due diligence before hiring data service providers; (2) have appropriate protections of data in their contracts with data service providers; and (3) take steps to verify that the data service providers are adequately protecting data.

The *GMR* case has a number of important implications. The *GMR* case indicates that organizations that hire data service providers may be directly at fault in many instances. The case solidifies the principle that companies have duties of data service provider management—in choosing, contracting with and overseeing vendors. This means that if a vendor has a problem, the organization that hired the vendor will also be under scrutiny.

---

of educational records to third parties but merely imposes a funding precondition such that an institution will not receive federal funding if the institution has a 'policy or practice of permitting the release of education records.' An institution, therefore, stands to lose all or a portion of its federal funding if it has a policy or practice of disclosing its students' educational records to unauthorized third parties.'' (quoting 20 U.S.C. § 1232g(b)(1)).

[6] 15 U.S.C. § 45(a)(1).

[7] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. (forthcoming 2014), *available at* http://ssrn.com/abstract=2312913.

[8] Complaint, *In re GMR Transcription Services, Inc.*, File No. 122 3095 (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140203gmrcmpt.pdf.

[9] Agreement Containing Consent Order, *In re GMR Transcription Services, Inc.*, File No. 122 3095 (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140203gmragree.pdf (13 PVLR 211, 2/3/14).

[10] GMR Complaint, *supra* note 8, at 3.

[11] *Id.* at 4.

[12] *Id.*

  PVLR ISSN 1538-3423

Organizations that use data service providers for data processing might not just be victims if the data service providers make a blunder. They might be to blame if they did not engage in appropriate data service provider management practices.

FTC enforcement based on inadequate data service provider management signals that standards in this area are starting to mature. The *GMR* case does not define the precise contours of what constitutes adequate data service provider management, but the details will be fleshed out over time. This FTC case has signaled that more attention should be devoted to the issue, and we can now expect more companies to take a closer look at their own data service provider management practices. The word is out that poor data service provider management might run afoul of the FTC Act. Even without a data breach, poor data service provider management alone might still be a cause for FTC enforcement.

Although the FTC generally cannot enforce against public-sector entities, the *GMR* case still has important implications. The case now establishes more clearly that there is a standard of care when it comes to contracting. The principles in this case apply to nearly all businesses, and FTC decisions reflect the consensus norms about privacy. If nearly all companies are legally obligated to do what the FTC demands in this decision, then this puts a lot more pressure on schools and other public-sector organizations to do so.

Protections of Third-Party Beneficiaries

The FTC is also not limited in protecting consumers only when they have a direct relationship with an entity that maintains their personal data. In its early cases, the FTC focused primarily on enforcing company privacy policies. But later on, the FTC broadened its enforcement far beyond privacy policies. Deception is a broad concept, and it is not limited to the explicit promises a company might make. Unfairness is even broader. An ''unfair'' trade practice is one that ''causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.''[13] An exceptionally wide range of activities has been included in the FTC's unfairness and regulatory efforts.[14] Many of the alleged unfair actions seek to take advantage of vulnerable consumers, making exploitation the locus of many unfairness allegations.[15] Thus, the FTC has very broad and general regulatory authority by design to allow for a more nimble and evolutionary approach to the regulation of consumer protection.

Because FTC enforcement is not tethered to any specific privacy policy and is primarily focused on protecting consumers, it becomes quite apparent that the FTC has the authority to regulate entities maintaining personal data even if those entities do not make any promises directly to the people to whom the data pertain.

In *In re Vision I Properties LLC*, the FTC brought an action against Vision I Properties, a company that provided software that created customized shopping cart pages for other companies.[16] Vision I rented people's personal data collected through its software to direct marketers. This was in violation of some of the privacy policies of the companies using Vision I's software. Even though Vision I was not violating its own privacy policy, the FTC concluded that it thwarted consumer expectations formed based upon the privacy policies of the other companies.[17]

The import of this case is that the FTC did not see this scenario as involving merely an arrangement between Vision I and other companies. Consumers were caught in the middle, and the FTC ensured that their interests would not be lost in the relationship. Consumers need not have a direct relationship to companies that cause them harm. Combining *Vision I* with *GMR* suggests that consumers can be harmed when the appropriate contractual protections are not included in agreements involving the sharing of personal data.

Additionally, the FTC has already developed a theory of data security that requires companies holding personal information to ensure that third-party recipients will safeguard any data the company shares.[18] Specifi-

[13] 15 U.S.C. § 45(n).

[14] *See Philip Morris, Inc.*, 82 F.T.C. 16 (1973) (respondent had distributed free sample razor blades in such a way that they could come into the hands of small children) (consent agreement); *Holland Furnace Co. v. FTC*, 295 F.2d 302 (7th Cir. 1961) (seller's servicemen dismantled home furnaces and then refused to reassemble them until the consumers had agreed to buy services or replacement parts); *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354 (1988) (unilateral imposition of fees in breach of a service contract); Press Release, FTC, FTC Charges Fitness Quest, Inc. With Making Deceptive Claims and Failing to Disclose a Safety Risk From Use of Its ''Gut Buster'' Exercise Device (Jan. 8, 1990), http://www.casewatch.org/ftc/news/1990/gutbust.shtml (''Breakage has allegedly caused substantial physical injury to consumers, and failure to disclose such a risk is alleged to be an unfair practice.'').

[15] *See, e.g., R.F. Keppel & Bro., Inc v. FTC*, 291 U.S. 304, 313 (1934) (finding unfairness where an action ''exploit[s] consumers, children, who are unable to protect themselves''); Statement of Basis and Purpose of Trade Regulation Rule 408, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8355 (July 2, 1964).

[16] Complaint, *In re Vision I Properties, LLC*, File No. 042 3068, Docket No. C-4135 (Apr. 26, 2005), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2005/04/050426comp0423068.pdf.

[17] Decision and Order, *In re Vision I Properties, LLC*, File No. 042 3068, Docket No. C-4135 (Apr. 26, 2005), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2005/04/050426do0423068.pdf.

[18] For examples of FTC critiques of inadequate third-party access control, *see, e.g.*, First Amended Complaint for Injunctive and Other Equitable Relief at 12, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.bloomberglaw.com/public/document/Federal_Trade_Commission_v_Wyndham_Worldwide_Corporation_et_al_Do/5 (12 PVLR 1946, 11/18/13); Complaint for Civil Penalties, Injunctive and Other Equitable Relief at 7, *United States v. Rental Research Servs., Inc.*, No. 0:09-cv-00524-PJS-JJK (D. Minn. Mar. 5, 2009), *available at* http://www.bloomberglaw.com/public/document/United_States_of_America_v_Rental_Research_Services_Inc_et_al_Doc (8 PVLR 396, 3/9/09); Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 5, *United States v. ValueClick, Inc.*, No. 2:08-cv-01711-MMM-RZ (C.D. Cal. Mar. 13, 2008), *available at* http://www.bloomberglaw.com/public/document/United_States_of_America_v_Valueclick_Inc_et_al_Docket_No_208cv01 (7 PVLR 414, 3/24/08); Complaint at 4–5, *In re Upromise, Inc.*, File No. 102 3116, Docket No. C-4351

cally, the FTC has filed complaints of unfairness against companies it alleged failed to verify and authenticate the identities of third-party recipients,[19] failed to monitor the data recipient's activity[20] and failed to require by contract third-party protection of information.[21] The FTC could adopt a similar approach with respect to privacy-based requirements, such as requirements for confidentiality and data minimization and prohibitions on re-identification, data mining and certain kinds of advertising and marketing to those identified.

The FTC's power to protect third-party beneficiaries of institutional bargaining extends to companies that provide cloud services to public-sector entities. Although the FTC can generally only regulate commercial entities under Section 5,[22] when public-sector institutions such as schools use private-sector cloud service providers, the FTC can regulate the cloud service provider. Although the cloud service provider might not have a direct relationship with the individuals whose data they maintain, these individuals are third-party beneficiaries of the privacy promises made by those who provide data to cloud service providers. So if a school enters into a contract with a cloud service provider where student data are shared with the provider, that provider must live up to consumer expectations. Moreover, if the provider negotiates a deficient contract with a school, the deficiencies in this arrangement might themselves be contrary to student expectations. As the FTC recognized in *GMR*, protecting privacy involves structuring relationships with cloud providers appropriately. There might be a reciprocal obligation on the part of the cloud service provider to structure the appropriate relationship with the entity supplying the data to ensure consumers are not harmed or misled.

As of this time, the FTC has not gone quite this far, but the foundations are present in its jurisprudence for it to start taking these steps. It takes two to tango, and the FTC has the principles in place to recognize this fact and enforce *GMR*-like standards on both sides of contracts with cloud service providers.

Cloud Service Providers as Data Stewards

The FTC has started to embrace a larger philosophy that third-party data service providers should act as data stewards. In other words, companies that collect, use and share personal data owe certain responsibilities to the data subjects. These responsibilities could include ensuring harm from the use and distribution of data is minimized through the use of technical safeguards, administrative procedures and contractual terms. Data stewardship is already a concept embraced in certain specific areas, such as health care. The FTC's approach draws upon the tradition of ''third-party beneficiaries'' in contract law, whereby intended third-party recipients of benefits of a contractual term are entitled to enforce that term even though they are not technically a party to the agreement.[23]

Good stewardship even has a fiduciary-like quality whereby relationships with stark disparities in power are sometimes treated differently than those who negotiate at arm's length. In this way, the FTC approach is similar to that of courts when finding implied obligations of confidentiality.[24] Consumers have very little ability to ensure that cloud service providers protect the personal data that were entrusted to them, which makes these consumers vulnerable and largely unable to reasonable avoid risk. The FTC has laid the foundations for establishing standards of data stewardship on each side of the cloud service relationship. The next steps have yet to be taken, but the path is there, waiting to be traversed.

(F.T.C. Mar. 27, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisecmpt.pdf (11 PVLR 61, 1/9/12); Complaint at 2, *In re ACRAnet, Inc.*, File No. 092 3088, Docket No. C-4331 (F.T.C. Aug. 17, 2011), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110809acranetcmpt.pdf (10 PVLR 188, 2/7/11); Complaint at 3–4, *In re Premier Capital Lending, Inc.*, File No. 072 3004, Docket No. C-4241 (F.T.C. Dec. 10, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/12/081206pclcmpt.pdf (7 PVLR 1603, 11/10/08); Complaint at 2, *Nations Title Agency, Inc.*, File No. 052 3117, Docket No. C-4161 (F.T.C. June 19, 2006), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/06/0523117nationstitle_complaint.pdf (5 PVLR 689, 5/15/06). This includes the failure to verify and authenticate the identities of third-party recipients as well as the failure to monitor or otherwise identify unauthorized recipient activity. *See* Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 4, *United States v. ChoicePoint Inc.*, No. 1:06-cv-00198-GET (N.D. Ga. Jan. 30, 2006), *available at* http://www.bloomberglaw.com/public/document/United_States_of_America_v_ChoicePoint_Inc_Docket_No_106cv00198_N (5 PVLR 110, 1/30/06) (discussing defective verification policies). It includes general charges of failing to protect information in the hands of third-party recipients as well as very specific charges by the FTC such as ''[f]ailing to oversee service providers and to require them by contract to implement safeguards to protect respondent's customer information.'' Nations Title Agency Complaint, *supra* note 18, at 4.

[19] *See, e.g.*, ChoicePoint Complaint, *supra* note 18, at 5 (admonishing company for accepting contradictory verification documentation).

[20] *See id.* at 9–10.

[21] This is also a violation of the Gramm-Leach-Bliley Act Safeguards Rule. *See, e.g.*, Complaint, *In re Sunbelt Lending Servs., Inc.*, File No. 042 3153, Docket No. C-4129 (Jan. 7, 2005), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2005/01/050107comp0423153.pdf (analyzing violations of Safeguards Rule) (3 PVLR 1316, 11/22/04); Nations Title Agency Complaint, *supra* note 18, at 3–4 (same).

[22] *Cal. Dental Ass'n v. FTC*, 526 U.S. 756, 766–67 (1999); *Community Blood Bank v. FTC*, 405 F.2d 1011, 1012 (8th Cir. 1969).

[23] Restatement (Second) of Contracts § 304 (1981); Woodrow Hartzog, *Promises and Privacy: Promissory Estoppel and Confidential Disclosure in Online Communities*, 82 Temp. L. Rev. 891, 928 (2009).

[24] Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 Ind. L.J. 763, 777–78 (2014) (''To courts, implied expectations of confidentiality were more plausible in developed relationships, unequal bargaining power could inhibit the ability of vulnerable parties to explicitly request confidentiality, and relationships formed in pursuit of a common goal required confidentiality to be effective. The courts' keen attention to vulnerability has yet to be as rigorously applied in most online environments.'')

  PVLR ISSN 1538-3423

Electronic copy available at: https://ssrn.com/abstract=2424998