Santa Clara High Technology Law Journal

Volume 29 | Issue 3 Article 1

4-23-2013

The Information Privacy Law of Web Applications and Cloud Computing

Sebastian Zimmeck

ARTICLES

THE INFORMATION PRIVACY LAW OF WEB APPLICATIONS AND CLOUD COMPUTING

Sebastian Zimmeck†

Abstract

This article surveys and evaluates the privacy law of web applications and cloud computing. Cloud services, and web applications in particular, are subject to many different privacy law requirements. While these requirements are often perceived as ill-fitting, they can be interpreted to provide a structurally sound and coherent privacy regime. The applicable body of law can be separated into two tiers: the primary privacy law and the secondary privacy law. The primary privacy law is created by the providers and users of cloud services through privacy contracts, especially, privacy policies. The secondary privacy law, contained, for example, in statutes and regulations, is for the most part only applicable where no valid privacy contracts exist. This supremacy of privacy contracts over statutory and other secondary privacy law enables individualized privacy protection levels and commercial use of privacy rights according to the contracting parties' individual wishes.

† Ph.D. candidate (Computer Science), Columbia University; M.S. (Computer Science), Columbia University, 2011; Dr. iur., Christian-Albrechts-University Kiel, 2008; LL.M., University of California, Berkeley, 2006; First State Examination, Christian-Albrechts-University Kiel, 2003. I would like to thank Google and the University of California, Berkeley for a generous research fellowship that made this work possible. I am also thankful for the help of Gabriella E. Ziccarelli, Claudine Wong, Maxim V. Tsotsorin, Jessica Shafer, Andy Pierz, Daniel Perry, and Anne Mostad-Jensen of the Santa Clara Computer and High Technology Law Journal. Last but not least, my gratitude goes to Jie S. Li and Carrie R. Aeb. All views are my own.

TABLE OF CONTENTS

I. INTRODUCTION

This article surveys and evaluates the privacy law of web applications and cloud computing. The National Institute of Standards and Technology defines "cloud computing" as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1] Depending on which services are provided, three categories of cloud computing can be distinguished: software-as-a-service (applications), platform-as-a-service (foundational elements to develop applications), and infrastructure-as-a-service (computational and storage infrastructure).[2] Therefore, cloud computing services also cover web applications, such as webmail services, web search

1. PETER MELL & TIMOTHY GRANCE, U.S. DEPT. OF COMMERCE, NAT'L INST. OF STANDARDS AND TECH., SPECIAL PUB. NO. 800-145, THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

2. *See, e.g.*, Mache Creeger, *Cloud Computing: An Overview*, ACM QUEUE, June 1, 2009, at 1, *available at* http://queue.acm.org/detail.cfm?id=1554608. *But see, e.g.*, Michael Armbrust et al., *A View of Cloud Computing*, 53 COMM. OF THE ACM no. 4, Apr. 2010, at 50, 50, *available at* http://dl.acm.org/citation.cfm?id=1721672&bnc=1 ("The line between 'low-level' infrastructure and a higher-level 'platform' is not crisp. We believe the two are more alike than different, and we consider them together.").

services, and social networks.[3] They are subject to the same considerations as other cloud computing services and accordingly addressed in this article.

The privacy law of cloud computing can be separated into two tiers. The primary privacy law is created by privacy contracts, while the secondary privacy law follows from constitutional privacy rights, common law rules, statutes, and regulations.[4] By making use of privacy contracts, cloud service providers and users can shape their privacy relationship largely any way they want. Generally, they are subject to the secondary privacy law only to the extent they do not make use of privacy contracts. The reason for the supremacy of privacy contracts over the secondary privacy law is the constitutionally guaranteed freedom of contract. Thus, for example, a valid provision in a privacy contract can be understood as a user's consent to exclude an otherwise applicable privacy protection law.[5] The primary privacy law of cloud computing will be addressed in Part II. Part III will then describe the secondary privacy law. Lastly, Part IV will conclude with a few final remarks.

II. PRIMARY PRIVACY LAW OF CLOUD COMPUTING

From a formal perspective, a privacy contract binds only the contract parties.[6] However, because court decisions and regulatory enforcement actions can establish precedents and approved practices, privacy contracts can become relevant for third parties as well. Generally, cloud service providers and users can agree to any privacy arrangement they want. Privacy contracts can be explicit or implicit and, in the area of cloud computing, will often take the form of

3. *See, e.g.*, Muhammad Ali Babar & Muhammad Aufeef Chauhan, *A Tale of Migration to Cloud Computing for Sharing Experiences and Observations*, *in* PROCEEDINGS OF THE 2ND INT'L WORKSHOP ON SOFTWARE ENG'G FOR CLOUD COMPUTING, May 2011, at 50, 50 ("[M]ost of the state-of-the-art social networking applications such as Facebook, Twitter, YouTube, and Flickr are reported to be based on high-performance cloud platforms . . . .").

4. *See generally* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000) (discussing the contractual conception of information privacy law from a First Amendment perspective). *See also* Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559 (2000) (responding to Eugene Volokh's discussion of information privacy law).

5. *See, e.g.*, 18 U.S.C. § 2701(c)(2) (2011). *See also* § 2702(b)(3), (c)(2).

6. *See, e.g.*, Eugene Volokh, *Personalization and Privacy*, 43 COMM. OF THE ACM no. 8, Aug. 2000, at 84, 86 ("Contracts, however, have one important limitation: They legally constrain only the parties to the contract.").

service level agreements or be dependent on terms and conditions. The following section will discuss various aspects of privacy contracts between cloud service providers and users, in particular, contract formation, enforcement, and remedies. Thereafter, the next section will explore the extent to which privacy policies are equal to contracts, and how they can shape privacy relationships.

A. Privacy Contracts

Every enforceable contract requires valid contract formation,[7] which consists of an offer, acceptance, mutual assent, and consideration.[8] In many cases contract formation on the web happens through clickwrap and browsewrap mechanisms. A cloud service provider using a clickwrap or browsewrap mechanism would display the contract terms on its website for the user to accept by clicking on a button or browsing the website, respectively. For both mechanisms valid contract formation often hinges on mutual assent. *ProCD v. Zeidenberg* addressed a clickwrap mechanism and found the click on a button before software could be used sufficient to indicate assent to the terms of the software license.[9] Other courts presented with the issue followed *ProCD* and focused on whether the users had reasonable notice of the terms of the contracts in question.[10] Different from a clickwrap mechanism, in case of a browsewrap mechanism the user's assent to the cloud service provider's contract offer depends on the mere use of the service.[11] In this regard, some courts and commentators suggest that contract formation can be more easily

7. *See, e.g.*, Nancy S. Kim, *The Software Licensing Dilemma*, 2008 BYU L. REV. 1103, 1136 ("Whether the written terms are binding as an agreement upon the parties depends on whether there was valid contract formation and no invalidating circumstances (such as unconscionability or duress).").

8. *Id.* at 1124.

9. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1452 (7th Cir. 1996) ("A vendor, as master of the offer, may invite acceptance by conduct . . . . A buyer may accept by performing the acts the vendor proposes to treat as acceptance."). *See also* U.C.C. § 2-204(1) (2011) ("A contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract.").

10. *See, e.g.*, Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 30-32, 35 (2d Cir. 2002); Feldman v. Google, Inc. 513 F. Supp. 2d 229, 236-238 (E.D. Pa. 2007); I. Lan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328, 336 (D. Mass. 2002); Forrest v. Verizon Commc'ns, Inc., 805 A.2d 1007, 1010 (D.C. 2002).

11. Allyson W. Haynes, *Web Site Visitors and Online Privacy: What Have You Agreed to Share?*, 20 S.C. LAW., July 2008, at 27, 30, *available at* http://works.bepress.com/cgi/viewcontent.cgi?article=1006&context=allyson_haynes.

inferred for businesses than for consumers.[12]

In *Specht v. Netscape* the court addressed mutual assent for browsewrap agreements and held that where consumers can download software at the click of a button, a reference to the existence of license terms on a submerged screen is insufficient to place consumers on notice of those terms.[13] The court found that the download website screen was designed in such a manner that it tended to conceal the fact that it was an express acceptance of Netscape's rules and regulations.[14] In order to be bound to a browsewrap agreement and infer mutual assent many courts mandate that users must have actual or constructive knowledge of a service's terms and conditions prior to using the service.[15] Constructive knowledge requires that users are able to see the link to the terms and conditions without scrolling down to the bottom of the screen.[16]

The question of when a link to terms and conditions is sufficiently designed to infer a user's constructive knowledge is dependent on the individual circumstances of the case. One court found it sufficient that a website stated that "[b]y submitting [information] you agree to the Terms of Use" next to a blue hyperlink for access to those terms.[17] Another court, however, noted that

---

12. *See, e.g.*, Fteja v. Facebook, Inc., 841 F. Supp. 2d 829, 836 (S.D.N.Y. 2012) ("Moreover, the cases in which courts have enforced browsewrap agreements have involved users who are businesses rather than . . . consumers."); Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMM. L. & POL'Y 405, 419 (2010) (describing that courts see businesses as more sophisticated than consumers when entering into online contracts); Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 472 (2006) ("An examination of the cases that have considered browsewraps in the last five years demonstrates that the courts have been willing to enforce terms of use against corporations, but have not been willing to do so against individuals.").

13. *See Specht*, 306 F.3d at 32. *See also* Jennifer Femminella, Note, *Online Terms and Conditions Agreements: Bound by the Web*, 17 ST. JOHN'S J. LEGAL COMMENT. 87 (2003) (arguing that browsewrap agreements are unenforceable). *But see Fteja*, 841 F. Supp. 2d at 839.

14. *Specht*, 306 F.3d at 32 (citing Larrus v. First Nat'l Bank of San Mateo Cnty, 266 P.2d 143, 147 (1954)).

15. *See, e.g.*, *Specht*, 306 F.3d at 31; Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 937 (E.D. Va. 2010) (citing Sw. Airlines Co. v. BoardFirst, LLC, No. 3:06-CV-0891-B, 2007 WL 4823761, at *5 (N.D. Tex. Sept. 12, 2007)); Hines v. Overstock.com, Inc., 668 F. Supp. 2d 362, 367 (E.D.N.Y. 2009) (citing *Sw. Airlines Co.*, 2007 WL 4823761, at *5); *Sw. Airlines Co.*, 2007 WL 4823761, at *5 (citing Lemley, *supra* note 12, at 477; Tarra Zynda, Note, *Ticketmaster Corp. v. Tickets.com, Inc.: Preserving Minimum Requirements of Contract on the Internet*, 19 BERKELEY TECH. L.J. 495, 507 (2004)); Ticketmaster Corp. v. Tickets.com, Inc., No. CV997654HLHVBKX, 2003 WL 21406289, at *2 (C.D. Cal. Mar. 7, 2003).

16. *Hines*, 668 F. Supp. 2d at 367.

17. *See* Major v. McCallister, 302 S.W.3d 227, 230-31 (Mo. Ct. App. 2009). *See also*

constructive knowledge is difficult to infer if a hyperlink to the terms appeared in small gray print on a gray background.[18] Similarly, another court has declined to enforce terms and conditions that "only appear[ed] on [a] website via a link buried at the bottom of the first page."[19] In general, constructive knowledge can be inferred if the cloud service provider uses a conspicuous design for the link and provides access to the full terms and conditions upon clicking the link.

In Maryland and Virginia clickwrap and browsewrap contract formation is governed by the Uniform Computer Information Transactions Act (UCITA),[20] though formation under this statute is not materially different than in the other states. Under Maryland and Virginia law, mutual assent in case of clickwrap or browsewrap contract formation requires that a person has had an "opportunity to review" the terms and intentionally "engages in conduct or makes statements with reason to know that the other party . . . may infer from the conduct or statement that the person assents" to the terms of the contract.[21] Individuals, however, are only deemed to have had an "opportunity to review" a contract term if it is "available in a manner that ought to call it to the attention of a reasonable person and permit review."[22]

While contract formation generally requires mutual assent,[23]

Fteja, 841 F. Supp. 2d at 840 (citing *Major*, 302 S.W.3d at 229-31); Cairo, Inc. v. Crossmedia Servs., Inc., No. C 04-04825 JW, 2005 WL 756610, at *2, *5 (N.D. Cal. 2005) (finding sufficient that a website displayed the notice "By continuing past this page and/or using this site, you agree to abide by the *Terms of Use* . . . ," with "Terms of Use" being an underlined and highlighted hyperlink leading to the actual terms).

18. Pollstar v. Gigmania Ltd., 170 F. Supp. 2d 974, 981 (E.D. Cal. 2000).

19. *Cvent, Inc.*, 739 F. Supp. 2d at 936–37 (E.D. Va. 2010). *But see Fteja*, 841 F. Supp. 2d at 836 (citing *Cvent, Inc.*, 739 F. Supp. 2d at 937–38); Koch Indus. v. Doe, No. 2:10CV1275DAK, 2011 U.S. Dist. LEXIS 49529, at *21-26 (D. Utah May 9, 2011) (citing *Cvent, Inc.*, 739 F. Supp. 2d at 936–37).

20. More specifically, UCITA "applies to computer information transactions." MD. CODE ANN., COMMERCIAL LAW § 22-103(a) (West 2012); VA. CODE ANN. § 59.1-501.3(a) (West 2012).

21. MD. CODE ANN., COMMERCIAL LAW § 22-112(a)(2); VA. CODE ANN. § 59.1-501.12(a)(2).

22. MD. CODE ANN., COMMERCIAL LAW § 22-112(e)(1); VA. CODE ANN. § 59.1-501.13:1(a).

23. *See* Dyer v. Nw. Airlines Corp., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) ("[B]road statements of company policy do not generally give rise to contract claims.") (citing Martens v. Minn. Mining & Mfg. Co., 616 N.W.2d 732, 740 (Minn. 2000) (en banc); Pratt v. Heartview Found., 512 N.W.2d 675, 677 (N.D. 1994)); *In re* Nw. Airlines Privacy Litig., No. 04-126

promissory estoppel provides an exception to this principle based on detrimental reliance.[24] Under the doctrine of promissory estoppel, a "promise which the promisor should reasonably expect to induce action or forbearance on the part of the promisee or a third person and which does induce such action or forbearance is binding if injustice can be avoided only by enforcement of the promise."[25] Such promise "is a contract, and full-scale enforcement under normal remedies is often appropriate."[26] Thus, for example, an enforceable contract can be created if a cloud service provider promises to not disclose information and users provide information in reliance on that promise.[27] In such case promissory estoppel can be available, independent of mutual assent, to the extent the users "accessed, read, understood," and "actually relied upon" the promise.[28]

A particularly relevant defense against enforcement of privacy contracts is the doctrine of unconscionability, which is used to counter unfair or one-sided contracts.[29] In most states, it has a procedural and a substantive component.[30] The procedural component

(PAM/JSM), 2004 U.S. Dist. LEXIS 10580, at *16-17 (D. Minn. June 6, 2004) (explaining that privacy policies are generally not contractual and that the policy at issue lacked definiteness, acceptance, and reliance, which are required for contract formation).

24. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 3 (2011) ("Promises to protect privacy might be enforced through promissory estoppel.").

25. RESTATEMENT (SECOND) OF CONTRACTS § 90(1) (1981).

26. *Id.* § 90 cmt. d.

27. *See* Volokh, *supra* note 6, at 86 ("If the site says 'We promise to keep your data private,' and people act in reliance on that promise, that promise becomes a binding contract."). *See also* RAYMOND T. NIMMER, 1 INFORMATION LAW § 8:79 (2012) ("Privacy rights between private parties can be created by contract or representations.").

28. *See Dyer*, 334 F. Supp. 2d at 1200. *See also In re Nw. Airlines Privacy Litig.*, 2004 U.S. Dist. LEXIS 10580, at *14-17 ("Plaintiffs do not contend that they actually read the privacy policy prior to providing Northwest with their personal information.").

29. *See* RESTATEMENT (SECOND) OF CONTRACTS § 208 (1981); U.C.C. § 2-302 (2011); Daniel J. Gervais & Daniel J. Hyndman, *Cloud Control: Copyright, Global Memes and Privacy*, 10 J. ON TELECOMM. & HIGH TECH. L. 53, 86 (2012) (discussing the "abuse of bargaining position that major Cloud service companies can try to exert over their users"); Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587, 618-19 (2007); John Soma et al., *Chasing the Clouds Without Getting Drenched: A Call for Fair Practices in Cloud Computing Services*, 16 J. TECH. L. & POL'Y 193, 211 (2011) ("Given their size and bargaining power, cloud services providers are in a position to dictate terms that are favorable to themselves, but risky for consumers.").

30. *See In re* iPhone Application Litig., No. 11–MD–02250–LHK, 2011 WL 4403963, at *7 (N.D. Cal. Sept. 20, 2011) (citing Armendariz v. Found. Health Psychcare Servs., Inc., 6 P.3d 669, 690 (Cal. 2000)); Feldman v. Google, Inc., 513 F. Supp. 2d 229, 239 (E.D. Pa. 2007) (citing Blake v. Ecker, 113 Cal. Rptr. 2d 422, 433 (Ct. App. 2001)); Haynes, *supra* note 29, at 619.

is satisfied by the existence of unequal bargaining positions or hidden terms.[31] Thus, a contract or some of its terms may be procedurally unconscionable if it is a contract of adhesion.[32] "A contract of adhesion is a form or standardized contract prepared by a party of superior bargaining power, to be signed by the party in the weaker position, who only has the opportunity to agree to the contract or reject it, without an opportunity to negotiate or bargain."[33] This can be the case if cloud services are not interchangeable. For example, a user of a social network may be only able to connect to his or her friends on one particular network and, hence, be dependent on using it. If the substantive component would also be satisfied, that is, enforcing the contract would lead to "overly harsh or one-sided results that 'shock the conscience,'"[34] the doctrine of unconscionability would prevent such enforcement.

Addressing damages, for breaches of privacy contracts, a proof of damages can be difficult. The loss of privacy as such is not a sufficient damage.[35] Information does not constitute property and accordingly cannot be damaged.[36] Personally identifiable information (PII) as such—for example, an individual name—does not have a compensable value.[37] Receiving and disclosing information that is otherwise not public can, however, be a benefit and, thus, could arguably be subject to unjust enrichment.[38] But in states where unjust enrichment is a quasi-contractual claim, plaintiffs may be barred from

---

31. *See In re iPhone Application Litig.*, 2011 WL 4403963, at *7; *Feldman*, 513 F. Supp. 2d at 239 (citing Comb v. PayPal, Inc., 218 F. Supp. 2d 1165, 1172 (N.D. Cal. 2002)); Haynes, *supra* note 29, at 619.

32. *See Feldman*, 513 F. Supp. 2d at 240 (citing Flores v. Transamerica HomeFirst, Inc., 113 Cal. Rptr. 2d 376, 382 (Ct. App. 2001)); Haynes, *supra* note 29, at 619-20.

33. *See Feldman*, 513 F. Supp. 2d at 240 (citing *Armendariz*, 6 P.3d at 689).

34. *See id.* at 239 (quoting *Comb*, 218 F. Supp. 2d at 1172).

35. *See* Trikas v. Universal Card Servs. Corp., 351 F. Supp. 2d 37, 46 (E.D.N.Y. 2005).

36. *See In re* Facebook Privacy Litig., 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011) (citing Thompson v. Home Depot, Inc., No. 07cv1058 IEG (WMc), 2007 U.S. Dist. LEXIS 68918, at *3 (S.D. Cal. Sept. 18, 2007)).

37. *See* Stayart v. Google Inc., 783 F. Supp. 2d 1055, 1057 (E.D. Wis. 2011); *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005).

38. *See, e.g.*, *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1075 (N.D. Cal. 2012); Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 815 (N.D. Cal. 2011); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d at 718; *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d at 329-30; Class Action Complaint at 57, Lane v. Facebook, Inc., 696 F.3d 811 (9th Cir. 2012) (No. C08 03845 RS), 2008 WL 3886402, paras. 178-81.

making such a claim if they also make a contractual claim.[39] In general, privacy remedies for personal wrongs are not easily accommodated within the existing legal regime.[40] In this regard, it can be difficult to show damages for a violation of a privacy contract.

B. Privacy Policies

"Privacy policies are written statements of company practices with respect to the treatment of personal data of website visit[o]rs."[41] If a user assents to or detrimentally relies on such a statement, a privacy policy can be a valid privacy contract. However, this is not always the case and depends on the individual circumstances.[42] The policy must meet the requirements for contract formation and enforcement, as described in the previous section. Thus, if a privacy policy does not provide a mechanism for obtaining the user's affirmative consent, which is usually the case, contract formation

---

39. *See, e.g.*, *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1075-76 (citing McBride v. Boughton, 20 Cal. Rptr. 3d 115, 122 (Ct. App. 2004)); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d at 718 (citing Villager Franchise Sys., Inc. v. Dhami, Dhami & Virk, No. CVF046393RECSMS, 2006 WL 224425, at *7 (E.D. Cal. Jan. 26, 2006)).

40. *See* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 890-92 (2003). *See generally* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1142-55 (2011) (describing "the outer boundaries and core properties of [a] privacy harm").

41. Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2043 n.6 (2000). *See also* FED. TRADE COMM'N, PROTECTING CHILDREN'S PRIVACY UNDER COPPA: A SURVEY ON COMPLIANCE B-9 (2002), *available at* http://www.ftc.gov/os/2002/04/coppasurvey.pdf ("A 'Privacy Policy' is defined as a comprehensive description of the site's information practices—what the site does with the personal identifying information it collects from visitors to the site.").

42. *See generally In re* Nw. Airlines Privacy Litig., No. 04-126 (PAM/JSM), 2004 U.S. Dist. LEXIS 10580, at *16-17 (D. Minn. June 6, 2004) ("The usual rule in contract cases is that 'general statements of policy are not contractual.'" (quoting Martens v. Minn. Mining & Mfg. Co., 616 N.W.2d 732, 740 (Minn. 2000) (en banc))); Dyer v. Nw. Airlines Corp., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) (explaining that "broad statements of company policy do not generally give rise to contract claims") (citing Pratt v. Heartview Found., 512 N.W.2d 675, 677 (N.D. 1994); *Martens*, 616 N.W.2d at 740); RAYMOND T. NIMMER, LAW OF COMPUTER TECHNOLOGY § 17:68 (2012) ("Despite the lack of a bilateral offer and acceptance, privacy policies may become part of a contractual arrangement . . . ."); SOLOVE & SCHWARTZ, *supra* note 24, at 3 ("Confidentiality or other privacy protections can be an express or implied contractual term in a relationship."); Haynes, *supra* note 29, at 613-18 (viewing the enforcement of privacy policies as contract enforcement); Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. INTELL. PROP. L. 57, 91-92 (1999) (discussing the categorization of privacy policies as contracts); Walter W. Miller, Jr. & Maureen A. O'Rourke, *Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card?*, 38 HOUS. L. REV. 777, 795-803 (2001) (discussing the categorization of privacy policies as contracts).

rests on the principles developed for browsewrap contracts. If the browsewrap mechanism is sufficient, a privacy policy is a contract.[43] Therefore, privacy policies cannot be qualified as contracts solely based on their nature as privacy policies, but rather such qualification is dependent on the application of ordinary contract law principles. However, as the contract formation requirements of browsewrap agreements are very similar to the Federal Trade Commission's (FTC's) "clear and prominent notice" standard for posting privacy policies,[44] every privacy policy that complies with the FTC standard is also a contract. Thus, in practice, the vast majority of privacy policies are privacy contracts.

Generally, cloud service providers can decide whether or not they want to adopt a privacy policy.[45] However, there are certain exceptions that obligate them to have one. At the federal level, the Children's Online Privacy Protection Act (COPPA) requires a privacy policy if a service is directed to children or its provider knowingly collects children's personal information.[46] If a provider wants to collect, use, or disclose children's personal information, it must also obtain verifiable parental consent.[47] At the state level, California's Online Privacy Protection Act (OPPA) requires service providers to have a privacy policy if they collect PII from and about consumers

43. While not every privacy policy is a contract, every written privacy contract can be understood as a privacy policy. After all, such contracts are statements regarding a service provider's practices about the treatment of personal data. *See* NIMMER, *supra* note 42, § 17:68 ("Beyond contract analyses, online privacy statements may be regarded as statements about how the provider does business.").

44. The FTC standard consists of "placing a clear and prominent hyperlink or button labeled PRIVACY NOTICE or PRIVACY POLICY on [the] home page, and at each location on the site at which personal identifying information is collected, which directly links to the privacy notice screen(s) containing the required information." *See* Stipulated Consent Agreement and Final Order, FTC v. Rapp, No. 99-WM-783 (D. Col. June 23, 2000); Stipulated Consent Agreement and Final Order, FTC v. ReverseAuction.com, Inc., No. 1:00-cv-0032 (D.D.C. Jan. 10, 2000).

45. *See* NIMMER, *supra* note 27, at § 8:79 ("[T]here is no nationally applicable law of general application that requires the creation of privacy policies in the U.S. . . . ."). *See also* Hetcher, *supra* note 41, at 2055-56 ("[I]n principle, [the FTC] could bring enforcement actions against websites merely on the basis of 'unfair' practices.").

46. *See* 15 U.S.C. § 6502(b)(1)(A)(i) (2011); 16 C.F.R. §§ 312.3(a), 312.4(b) (2012). Although further federal laws require providers of certain services to give notice of their privacy practices, those same federal laws do not mandate that service providers post a privacy policy on their website. *See, e.g.*, 15 U.S.C. § 6803, 16 C.F.R. pt. 313 (applying to financial institutions); 45 C.F.R. § 164.520 (applying to health care providers and other covered entities).

47. 15 U.S.C. § 6502(b)(1)(A)(ii); 16 C.F.R. §§ 312.3(b), 312.5.

residing in California.[48] Furthermore, some state statues mandate a privacy policy for service providers that collect social security numbers.[49] If service providers voluntarily decide to have a privacy policy or are required to have one, they must only describe what they do with the PII of their users.[50] Information that is not PII does not need to be covered in privacy policies.[51] The FTC defines PII to mean "individually identifiable information from or about an individual consumer," such as a name, an email address, or an Internet protocol (IP) address.[52] Similar definitions are contained in COPPA and OPPA.[53]

Sometimes information is only identifying in certain instances. For example, depending on their content, sometimes search queries identify a particular person, while sometimes they do not.[54] Furthermore, a piece of information may only be identifying if it is aggregated with other information. Thus, while a single search query may not identify a particular person, an aggregation of many search queries may reveal habits, interests, and much more about an individual finally identifying it. Given these characteristics, it is debated whether search queries are PII or non-PII.[55] A similar

48. CAL. BUS. & PROF. CODE §§ 22575(a) (West 2012).

49. *See, e.g.*, MICH. COMP. LAWS ANN. § 445.84 (West 2012); CONN. GEN. STAT. ANN. § 42-471(b) (West 2012).

50. For a new concept of PII, see Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011). *See also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010) (arguing for abandoning the concept of PII altogether).

51. *See* Schwartz & Solove, *supra* note 50, at 1816 ("Information that falls within th[e] category [of PII] is protected, and information outside of it is not.").

52. *See, e.g.*, Decision and Order, *In re* Eli Lilly & Co., FTC Docket No. C-4047 (May 8, 2002). *See also* Decision and Order, *In re* Google Inc., FTC Docket No. C-4336, at 3 (Oct. 13, 2011) (defining "[c]overed information"); Decision and Order, *In re* of ACRAnet, Inc., FTC Docket No. C-4331, at 2 (Aug. 17, 2011) (defining "[p]ersonal information"); Decision and Order, *In re* Superior Mortg. Corp., FTC Docket No. C-4153, at 2 (Dec. 14, 2005) (defining "[p]ersonal information"); Decision and Order, *In re* Guess?, Inc., FTC Docket No. C-4091, at 2 (July 30, 2003) (defining "[p]ersonal information"); *Ex Parte* Temporary Restraining Order, FTC v. Prophet 3H, Inc., No. 06 CV 1692, at 6-7 (N.D. Ga. July 18, 2006) (defining "'[p]ersonally identifiable information' or 'identity information'").

53. 15 U.S.C. § 6501(8) (2011); CAL. BUS. & PROF. CODE § 22577(a).

54. *See* Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV. 1433, 1450 (2008) ("Depending on their intended uses, search-query logs may raise serious privacy problems.").

55. *See* Schwartz & Solove, *supra* note 50, at 1847-48 (arguing that the question of whether search queries are PII cannot be answered in the abstract).

question arises with regard to IP addresses.[56] Thus, it could be argued that certain types of information simply cannot be categorized as either PII or non-PII. However, the concept of PII inherently accounts for the uncertainty of the identification of an individual. Information is categorized as PII if it makes an individual *identifiable*, that is, there is a possibility of identifying the individual. It is not necessary that the individual is actually *identified*. In this regard, search queries and IP addresses are not different from names or postal addresses, which also do not necessarily identify an individual. Thus, information is PII if it is possible, perhaps together with other information, to identify a particular individual.

Privacy policies only need to describe privacy practices where PII is collected *from* and *about* an individual. This point is made expressly clear in OPPA's definition of PII which states that "[t]he term 'personally identifiable information' means individually identifiable information *about* an individual consumer collected online by the operator *from* that individual . . . ."[57] Similarly, it also follows from COPPA's definition of personal information as "individually identifiable information *about* an individual"[58] in combination with its prohibition to "collect personal information *from* a child."[59] Thus, obtaining PII about an individual from a third party does not create a privacy policy obligation vis-à-vis the individual. Rather, the individual released the information to the third party at his or her own risk, though the third party may have had an obligation to adopt a privacy policy and describe its information disclosure

56. *See, e.g.*, VPR Internationale v. Does 1-1017, No. 11-2068, 2011 U.S. Dist. LEXIS 64656, at *4 (C.D. Ill. Apr. 29, 2011) (noting the difficulty of correlating IP addresses to individual persons); Johnson v. Microsoft Corp., No. C06-0900RAJ, 2009 U.S. Dist. LEXIS 58174, at *12-13 (W.D. Wash. June 23, 2009) (holding that an IP address is not PII because it identifies a particular computer instead of an individual person); Columbia Pictures Indus. v. Bunnell, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *3 n.10 (C.D. Cal. May 29, 2007) (expressing doubt that an IP address can be PII because it identifies a particular computer instead of an individual person); Klimas v Comcast Cable Commc'ns, Inc., No. 02-CV-72054-DT, 2003 U.S. Dist. LEXIS 27765, at *10 (E.D. Mich. July 1, 2003) (holding that a dynamic IP address is not PII because it can be assigned to different persons), *aff'd on other grounds*, 465 F.3d 271 (6th Cir. 2006); Ben G. Isaacson, *Integrating Non-Personal Web Behavior with Personal Information*, 970 PLI/PAT 593, 599 (2009) (arguing that IP addresses cannot be considered personal information unless correlated with offline personal information); Tene, *supra* note 54, at 1446 ("The answer depends on whether the address might be linked to a specific individual through reasonable means.").

57. CAL. BUS. & PROF. CODE § 22577(a) (emphasis added).

58. 15 U.S.C. § 6501(8).

59. *Id.* § 6502(a)(1).

practices.[60] The requirement that information must be collected from and about an individual excludes a lot of information from being PII. For example, information about an individual posted on a social network by a third party is not PII of that individual.

If cloud service providers are required or voluntarily decide to have a privacy policy, the FTC Act generally allows them to determine what they want do with collected PII.[61] As long as they give sufficient notice thereof, they are generally free to treat the information any way they want.[62] Thus, to a large extent, the FTC's privacy policy enforcement focuses on the providers' compliance with the terms of their own privacy policies. If PII is collected, the FTC requires cloud service providers to adhere to their representations about information collection,[63] disclosure,[64] use,[65] and management.[66] Not providing a sufficient privacy policy can constitute an unfair or deceptive act or practice in or affecting

60. As the FTC definition of PII refers to information "from or about an individual," *supra*, note 52, it is not sound and should not be applied to that extent.

61. *See* Haynes, *supra* note 11, at 29 ("[T]he focus of FTC and state enforcement is primarily on the Web site's adherence to its promises, not a general standard of fairness.").

62. *Id.*; Haynes, *supra* note 29, at 588.

63. *See, e.g.*, Complaint at 3, *In re* ScanScout, Inc., FTC Docket No. C-4344 (Dec. 14, 2011) (alleging misrepresentation that consumers could opt out from receiving cookies thereby preventing information collection); Complaint at 5, *In re* Sears Holdings Mgmt. Corp., FTC Docket No. C-4264 (Aug. 31, 2009) (alleging misrepresentation about the extent to which a client-side application collects and transmits information); Complaint at 3, *In re* Microsoft Corp., FTC Docket No. C-4069 (Dec. 20, 2002) (alleging misrepresentation that no PII is collected).

64. *See, e.g.*, Complaint at 5-6, *In re* Myspace LLC, FTC Docket No. C-4369 (Aug. 30, 2012) (alleging misrepresentation about disclosure of user profiles and other PII); Complaint at 2-3, *In re* Vision I Properties, LLC, FTC Docket No. C-4135 (Apr. 19, 2005) (alleging misrepresentation about disclosure of shopping information and other PII); Complaint, *In re* Eli Lilly & Co., FTC Docket No. C-4047 (May 8, 2002) (alleging misrepresentation about disclosure of email addresses).

65. *See, e.g.*, Complaint at 5, *In re* Google Inc., FTC Docket No. C-4336 (Oct. 13, 2011) (alleging misrepresentation by claiming that user information would be only used for webmail purposes, while it was also used to populate social network); Complaint, *In re* GeoCities, FTC Docket No. C-3850 (Feb. 5, 1999) (alleging misrepresentation by claiming that user information would only be used for the purpose of providing specific email advertising and other requested offers, while it was also used for other marketing purposes).

66. *See, e.g.*, Complaint at 6-7, *In re* Facebook, Inc., FTC Docket No. C-4365 (July 27, 2012) (alleging misrepresentation that users could restrict third parties' access to their profile information); Complaint at 5, *In re* Upromise, Inc., FTC Docket No. C-4351 (Mar. 27, 2012) (alleging misrepresentation that the toolbar would transmit information in an encrypted format); Complaint at 4, *In re* Guess?, Inc., FTC Docket No. C-4091 (July 30, 2003) (alleging misrepresentation that information is stored in an encrypted format).

commerce according to 15 U.S.C. § 45(a)(1) and may also be subject to state unfair competition laws. It can also be false advertisement according to 15 U.S.C. § 52.[67] Further, the FTC views the providers' failure to abide by self-regulatory programs they joined as violation of 15 U.S.C. § 45.[68]

Some state statues go beyond the FTC Act. Particularly, OPPA contains some detailed requirements for privacy policies. It mandates provision of a description of any available process for reviewing and requesting changes to any PII that is collected as well as of the process by which the provider notifies users of material changes to the privacy policy.[69] Therefore, to the extent that California residents are not excluded from a service, OPPA is the true measure of when and how to implement a privacy policy.[70] More generally, cloud service providers with a single nationally applicable privacy policy must default to the more stringent state law requirements. In this regard, the state law with the most stringent requirements will set the standard. If cloud service providers want to avoid such standard, they would need to provide state-specific privacy policies or even implement state-specific versions of their services.

---

67. *See generally* Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 816-17 (2011) (discussing that the main sources of FTC enforcement are 15 U.S.C. §§ 45 and 52).

68. *See*, *e.g.*, Complaint for Civil Penalties and Other Relief at 11-12, United States v. Google Inc., No. CV 12-04177 HRL (N.D. Cal. Aug. 8, 2012) (alleging misrepresentation by not disclosing the information collection and use practices contrary to a self-regulatory program). *See also* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 14, 73 (2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf ("The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join."); Laura J. Bowman, *Pulling Back the Curtain: Online Consumer Tracking*, 7 I/S: J. L. & POL'Y FOR INFO. SOC'Y 718, 737-38 (2012). Compliance with COPPA regulations will be assumed if the operator complies with self-regulatory guidelines approved by the FTC according to 16 C.F.R. § 312.11 (2012).

69. *See* CAL. BUS. & PROF. CODE § 22575(b)(2)-(3) (West 2012).

70. *See* Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868, 895 (2009) ("The standard becomes a national, though not a federally adopted, standard, and it may create externalities even if no other state adopts a conflicting rule."); Isaacson, *supra* note 56, at 600 ("Also, because most websites do not exclude California residents from transacting or registering online, the law serves as a de facto requirement for all online marketers who collect personal information."); Sarah B. Kemble, *Privacy Policies: Is There Really a Choice Anymore?*, 16 S.C. LAW. 26, 28 (2004) ("Because the geographical location of the operator is irrelevant, for all practical purposes the OPPA has the scope and impact of a federal privacy law.").

III. SECONDARY PRIVACY LAW OF CLOUD COMPUTING

If cloud service providers and users do not enter into valid privacy contracts, secondary privacy law will apply as the default. Further, even if valid privacy contracts exist, some of the secondary privacy law remains applicable.[71] While comprehensive federal legislation would be possible, especially, because the Internet can be categorized as a channel or an instrumentality of interstate commerce,[72] the secondary privacy law is actually characterized by narrow laws targeted to protect privacy in certain limited areas.[73] As shown in Figure 1, privacy-relevant actions in the relationship between a cloud service provider and a user are the collection, disclosure, use, and management of information.[74] All of these actions are subject to unfair competition statutes, however, are also governed by more specific laws. In the following sections, the applicable secondary privacy law will be discussed for each action.[75]

---

71. One example is the rules on information management. *See infra* Part III.D.

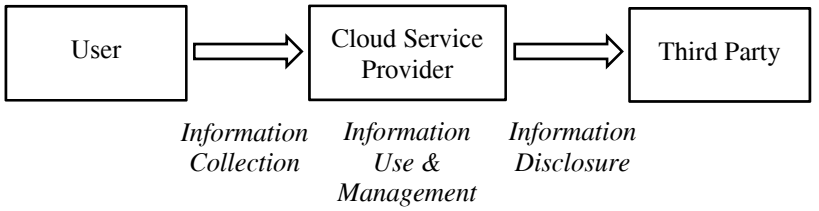
72. *See*, *e.g.*, United States v. Sutcliffe, 505 F.3d 944, 953 (9th Cir. 2007) (quoting United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (per curiam)) (holding that the Internet is an instrumentality and channel of interstate commerce); United States v. Hornaday, 392 F.3d 1306, 1311 (11th Cir. 2004) (citing Heart of Atlanta Motel, Inc. v. United States, 379 U.S. 241, 256 (1964); Brooks v. United States, 267 U.S. 432, 436 (1925)) ("Congress clearly has the power to regulate the internet, as it does other instrumentalities and channels of interstate commerce . . . ."); United States v. Penton, 380 F. App'x. 818, 820 (11th Cir. 2010) (citing *Hornaday*, 392 F.3d at 1311) (holding that the Internet is an instrumentality of interstate commerce).

73. Unlike the United States, many other countries enacted comprehensive privacy laws. For example, Canada's Personal Information Protection and Electronic Documents Act regulates the collection, use, and transfer of personal information by private organizations. *See* S.C. 2011, c. 5 (Can.). Likewise, Germany's Bundesdatenschutzgesetz (Federal Data Protection Act) covers the collection, processing, and use of PII by the government and private persons. *See* Bundesdatenschutzgesetz [Federal Data Protection Act], Jan. 14, 2003, BGBL. I at 66 (Ger.).

74. *See generally* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 490 fig.1 (2006) (providing an illustrative figure for the collection, processing, and dissemination of information as well as the invasions of privacy).

75. It is assumed that cloud service providers are private entities. In case of governmental cloud service providers or private providers acting as agents of the government, users would also have constitutional privacy rights against the providers. *See generally* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614 (1989) (citing United States v. Jacobsen, 466 U.S. 109, 113-14 (1984)) (holding that the Fourth Amendment applies if a private party acted as an instrument or agent of the government).

Figure 1. Privacy-Relevant Actions



A. Information Collection

Information collection means to obtain and store information from and about an individual. In order to collect information cloud service providers often access users' computers or install software on them, such as cookies, virtual machines, or browser extensions. These acts could allegedly violate the Stored Communications Act (SCA)[76]—particularly, 18 U.S.C. § 2701.[77] This provision penalizes the intentional accessing of an electronic communication facility without authorization or in excess of authorization and thereby obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage.[78] Some court decisions seem to argue that an individual user's computer is a "facility" and, thus, subject to 18 U.S.C. § 2701.[79] However, such application would be misguided.[80] First, the provision contains an exception for conduct authorized by the providers of wire or

76. 18 U.S.C. §§ 2701-2712 (2011).

77. *See*, *e.g.*, Class Action Complaint at 41, Lane v. Facebook, Inc., 696 F.3d 811 (9th Cir. 2012) (No. C08 03845 RS), 2008 WL 3886402, para. 115.

78. *See* § 2701(a).

79. *See*, *e.g.*, Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1160-61 (W.D. Wash. 2001) (concluding that it is possible to view users' computers as facilities protected by 18 U.S.C. § 2701); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1276 (C.D. Cal. 2001) (illustrating that a "'hacker' who accesses data in a computer without the owner's knowledge would be guilty of violating Section 2701"); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 508 (S.D.N.Y. 2001) (holding that accessing the communications of users to affiliated third parties can satisfy a claim under 18 U.S.C. § 2701); Expert Janitorial, LLC v. Williams, No. 3:09-CV-283, 2010 WL 908740, at *5 (E.D. Tenn. Mar. 12, 2010) (holding that unauthorized accessing of information on a computer can satisfy a claim under 18 U.S.C. § 2701).

80. *See In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1057-58 (N.D. Cal. 2012) (explaining that the decisions cited by plaintiff for the proposition that computers are "facilities" provide little insight because they assume this to be true and ultimately rule on other grounds).

electronic communications services.[81] Thus, if users' computers were covered by 18 U.S.C. § 2701, such providers would be authorized to grant third parties' access to users' computers, which would be an unusual result.[82] Therefore, a user's computer is not a "facility."[83] Second, according to 18 U.S.C. § 2701(a), the SCA prohibits obtaining, altering, or preventing authorized access with regard to communication in electronic storage, that is, communication in "temporary, intermediate storage" or "storage . . . for purposes of backup protection."[84] However, if only one copy of a communication exists—for example, one copy of an email on a user's hard drive—it is not covered because it is neither in temporary nor in backup storage. For the same reasons a permanently installed single software copy on a user's hard drive, such as a cookie, is not covered either.[85] Consequently, 18 U.S.C. § 2701 does not prohibit a cloud service provider from accessing a user's computer or installing software thereon.

However, cloud service providers are indeed subject to the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.[86] The CFAA essentially requires a provider to obtain the user's consent before installing any software on the user's computer.[87] Not obtaining consent can result in the provider's liability. Numerous states have spyware statutes comparable to the CFAA.[88] Therefore, as in the case of privacy policies,[89] cloud service providers must use a state-specific

81. *See* § 2701(c)(1).

82. *See In re iPhone Application Litig.*, 844 F. Supp. 2d at 1058 (citing Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1270-71 (N.D. Cal. 2001)).

83. *Id.*; *Crowley*, 166 F. Supp. 2d at 1271; Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1214-15 (2004).

84. § 2510(17).

85. *See In re iPhone Application Litig.*, 844 F. Supp. 2d at 1058-59 (citing *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 511; *In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *3 (N.D. Cal. Oct. 9, 2001)).

86. *See generally In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 520 (assuming that plaintiffs' computers were protected under the CFAA).

87. *See* 18 U.S.C. § 1030(a)(5)(A) (2011). *See also In re* Apple & ATTM Antitrust Litig., No. C 07-05152 JW, 2010 U.S. Dist. LEXIS 98270, at *26-27 (N.D. Cal. July 8, 2010) (holding that voluntary installation of software does not satisfy the requirement that the alleged act must be "without authorization" to be actionable under 18 U.S.C. § 1030(a)(5)(A)).

88. *See* SOLOVE & SCHWARTZ, *supra* note 24, at 123-24 (providing a comprehensive overview of state spyware statutes).

89. *See supra* Part II.B.

approach or accept the most restrictive state statute as setting the bar for compliance with spyware statutes.[90] However, civil actions under the CFAA are limited to certain enumerated circumstances.[91] In this regard, particularly, the $5,000 statutory minimum damages threshold has proven to be difficult to overcome for plaintiffs.[92] In addition to the CFAA and state spyware statutes, accessing of and installing software on a user's computer can be actionable under tort law as trespass to chattels.[93] If the user is not deprived from using the computer for a substantial time, however, the computer must be impaired as to its condition, quality, or value for trespass to chattels to apply.[94] Therefore, an action for trespass to chattels is generally limited to situations where the trespass actually did, or threatened to, interfere with the intended functioning of the computer, as by significantly reducing its available memory or processing power.[95]

For accessing a user's computer, installing software, and storing user information on a cloud service provider's server the intrusion upon seclusion tort must be considered as well.[96] In most states an intrusion does not have to be of a physically defined place, but can be of a person's personality or inner sphere.[97] However, the scope of intrusion upon seclusion is rather narrow because, as in any

90. Peter S. Menell, *Regulating "Spyware": The Limitations of State "Laboratories" and the Case for Federal Preemption of State Unfair Competition Laws*, 20 BERKELEY TECH. L.J. 1363, 1411 (2005).

91. § 1030(g), (c)(4)(A)(i).

92. § 1030(g), (c)(4)(A)(i)(I). *See generally* Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1158-59 (W.D. Wash. 2001); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1280-81 (C.D. Cal. 2001); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 520-26 (S.D.N.Y. 2001).

93. *See* RESTATEMENT (SECOND) OF TORTS §§ 216-222 (1965). For an argument of modernizing information privacy law by a unitary tort for invasion of privacy see Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CALIF. L. REV. 2007 (2010).

94. *See* RESTATEMENT (SECOND) OF TORTS § 218 (1965).

95. *See In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1069 (N.D. Cal. 2012) (citing Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1356 (2003)). *See also In re* Apple & ATTM Antitrust Litig., No. C 07-05152 JW, 2010 U.S. Dist. LEXIS 98270, at *26-27 (N.D. Cal. July 8, 2010) (voluntarily installed software eliminates a claim for trespass to chattels); Ticketmaster Corp. v. Tickets.com, Inc., No. CV997654HLHVBKX, 2003 WL 21406289, at *3 (C.D. Cal. Mar. 7, 2003) (holding that in the case of web crawling there must be some evidence that the use or utility of the affected computer is diminished thereby).

96. *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977).

97. *See, e.g.*, Phillips v. Smalley Maint. Servs., 435 So. 2d 705, 711 (Ala. 1983) ("One's emotional sanctum is certainly due the same expectations of privacy as one's physical environment.").

intentional tort, such claim can be defeated by consent, including consent that was improperly induced.[98] Thus, a court may be concerned with the scope of the consent and the extent to which a limited consent was exceeded.[99] In addition, the "highly offensive" requirement further narrows the tort's scope of application.[100] Therefore, in most cases the collection of information, such as names, addresses, social security numbers, purchasing, and financial transaction histories, will not be covered by this tort.[101]

B. Information Disclosure

Information disclosure means the forwarding of collected information from one party to another. Generally, cloud service providers are permitted to disclose information to whomever and in whatever way they want.[102] This right to disclose information is based on the First Amendment and also statutorily protected by the Communications Decency Act (CDA), 47 U.S.C. § 230.[103] However, the right is subject to restrictions.[104] Its limits depend on whether the

98. *See, e.g.*, Frye v. IBP, Inc., 15 F. Supp. 2d 1032, 1041 (D. Kan. 1998) (citing Baugh v. CBS, Inc., 828 F. Supp. 745, 757 (N.D. Cal. 1993)); *Baugh*, 828 F. Supp. at 757 (citing Cobbs v. Grant, 502 P.2d 1 (Cal. 1972)); Steven Perry, *Hidden Cameras, New Technology, and the Law*, 14 COMM. LAW. 1, 21 (1996).

99. *See* Perry, *supra* note 98, at 21.

100. RESTATEMENT (SECOND) OF TORTS § 652B (1977). *See, e.g.*, Boring v. Google Inc., 362 F. App'x. 273, 279 (3d Cir. 2010) (intruding upon the external view of the plaintiffs' premises cannot be considered highly offensive).

101. Candice L. Kline, Comment, *Security Theater and Database-Driven Information Markets: A Case for an Omnibus U.S. Data Privacy Statute*, 39 U. TOL. L. REV. 443, 463 (2008).

102. *See, e.g.*, Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011) (finding a Vermont law that generally prohibited disclosure and use of pharmacy records for marketing and promotion of prescription drugs an unconstitutional restriction of free speech); James Grimmelmann, *The Structure of Search Engine Law*, 93 IOWA L. REV. 1, 18-19 (2007) (arguing that a search engine is free to disclose collected information); Haynes, *supra* note 29, at 597 ("No law prevents a website operator from sharing or selling personal information it has lawfully been given . . . .").

103. *See generally* Stayart v. Google Inc., 783 F. Supp. 2d 1055, 1056 (E.D. Wis. 2011) ("The Communications Decency Act . . . effectively immunizes search engines like Yahoo and Google from claims that they displayed information created by third parties which presents an individual in an unfavorable light."), *aff'd*, No. 11-3012, 2013 WL 811793 (7th Cir. Mar. 6, 2013); Search King, Inc. v. Google Tech., Inc., No. CIV-02-1457-M, 2003 U.S. Dist. LEXIS 27193, at *11-12 (W.D. Okla. May 27, 2003) (ranking a website as displayed on a search results page is constitutionally protected speech). *But see* Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 801-03 (N.D. Cal. 2011) (holding that Facebook is not entitled to CDA immunity because it also provides its own content to users).

104. *See, e.g.*, Gonzales v. Google, Inc., 234 F.R.D. 674, 679-80 (N.D. Cal. 2006) (analyzing whether Rules 26(b) and 45 of the Federal Rules of Civil Procedure support a

cloud service provider discloses information to private parties or the government. The latter is much more restricted due to constitutional privacy rights of the user about whom information is disclosed. The following discussion will first describe the disclosure to private parties and then address disclosure to the government.

1. Disclosure to Private Parties

The most relevant provision for disclosure of information by cloud service providers to private parties is 18 U.S.C. § 2702. However, for the provision to be applicable an "electronic communication service" or "remote computing service" is required.[105] An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[106] In order to fall under this definition a cloud service provider must be "in the business of providing electronic communication services."[107] In other words, it must be the main purpose of the service to deliver electronic communications.[108] Examples of electronic communication services are webmail services,[109] social network services,[110] electronic bulletin board

subpoena requesting search query text).

105. 18 U.S.C. § 2702(a) (2011).

106. *Id.* § 2510(15).

107. *In re* Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 523-24 (N.D. Ill. 2011) (citing *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 307 (E.D.N.Y. 2005); Dyer v. Nw. Airlines Corp., 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004)). *See also* Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (holding that a licensor and supplier of petroleum refining, petrochemical, and gas processing technologies "is not in the business of providing electronic communication services").

108. *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d at 523-34. *See also In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d at 307 (holding that companies that provide traditional products and services over the Internet are not electronic communication service providers); Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001) (holding that an online merchant was not an electronic communication service provider even though it provides a platform for electronic communications in connection with its sales).

109. *See, e.g.*, Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 982 (C.D. Cal. 2010) (holding that webmail and social network services are electronic communication services); United States v. Weaver, 636 F. Supp. 2d 769, 770 (C.D. Ill. 2009) (holding that a webmail service is both an electronic communication service as well as remote computing service); Derek Constantine, Comment, *Cloud Computing: The Next Great Technological Innovation, the Death of Online Privacy, or Both?*, 28 GA. ST. U. L. REV. 499, 523 (2012) (arguing that webmail services should be categorized as electronic communication services).

110. *See, e.g.*, *Crispin*, 717 F. Supp. 2d at 982 (holding that webmail and social network services are electronic communication services).

services,[111] and computer reservation system services.[112] According to 18 U.S.C. § 2702(a)(1), providers of such services to the public are not allowed to disclose the contents of communications while in electronic storage. In this regard, the application of the provision often hinges on determining when communications are in "electronic storage."

"Electronic storage", as defined in the Wiretap Act[113] and applicable to the SCA, is "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[114] This twofold definition is somewhat limited. On the one hand, "temporary, intermediate storage" only covers communications not yet made available to the intended recipient.[115] On the other hand, storage "for purposes of backup protection" does not apply if only one copy of a communication exists.[116] Thus, for example, a webmail service ceases to provide electronic storage with regard to a particular email message upon the user's opening of this message.[117] However, if information is not or no longer in electronic storage, 18 U.S.C. § 2702 would remain applicable if the cloud service can be characterized as a remote computing service.

A "remote computing service" is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[118] Depending on the specific service, cloud services can qualify as remote computing services.[119]

---

111. *See, e.g.*, United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002).

112. United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993).

113. 18 U.S.C. §§ 2510–2522 (2011).

114. *Id.* § 2510(17).

115. *See, e.g.*, Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004) (citing *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 511-12 (S.D.N.Y. 2001)); *Crispin*, 717 F. Supp. 2d at 983 (citing *Theofel*, 359 F.3d at 1075).

116. *See, e.g.*, United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009) (holding that the storage of emails through a webmail service does not qualify as backup protection).

117. *Crispin*, 717 F. Supp. 2d at 985 (citing *Weaver*, 636 F. Supp. 2d at 772).

118. 18 U.S.C. § 2711(2).

119. *See* Matthew A. Goldberg, Comment, *The Googling of Online Privacy: Gmail, Search-Engine Histories and the New Frontier of Protecting Private Information on the Web*, 9 LEWIS & CLARK L. REV. 249, 272 (2005) (arguing that a search engine is a remote computing service). *But see* Matthew Werner, Comment, *Google and Ye Shall Be Found: Privacy, Search*

For example, courts found that publicly available webmail services,[120] video sharing services,[121] and social networks are remote computing services.[122] Thus, they are generally prohibited from disclosing communication contents. However, the prohibition may not always apply. The reason is that 18 U.S.C. § 2702(a)(2)(B) requires that the communication be transmitted to the service provider "solely for the purpose of providing storage or computer processing services" and that service providers must "not [be] authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing." Therefore, while many cloud services purposefully provide storage or computer processing services, if the service provider and the user agreed that the provider can access the communication contents of users, for example, for purposes of contextual advertising, such contents can be disclosed.[123]

So far it follows from the SCA that covered cloud service providers are generally not permitted to disclose the contents of communication.[124] The SCA, however, does not prohibit the disclosure of "a record or other information pertaining to a subscriber to or customer of such service (*not including the contents* of communications . . .) . . . to any person other than a governmental entity."[125] Thus, the law distinguishes between contents of communications and noncontent information.[126] To determine whether a cloud service provider is prohibited from disclosing to private parties information, such as search histories, one must decide if this information constitutes contents of communications.[127] The

---

Queries, and the Recognition of a Qualified Privilege, 34 RUTGERS COMPUTER & TECH. L.J. 273, 295 (2007) (arguing that a search engine is not a remote computing service).

120. *See, e.g.*, *Weaver*, 636 F. Supp. 2d at 770 (holding that a webmail service is both an electronic communication service as well as remote computing service).

121. Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008).

122. *See Crispin*, 717 F. Supp. 2d at 987, 990 (holding that a social network is a remote computing service with respect to opened and retained private messages as well as public wall postings and comments).

123. William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy under the Stored Communications Act*, 98 GEO. L.J. 1195, 1213-14 (2010). *See also* Ilana R. Kattan, Note, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 640 (2011).

124. 18 U.S.C. § 2702(a)(1), (2) (2011) (emphasis added).

125. *Id.* § 2702(c)(6) (emphasis added).

126. Goldberg, *supra* note 119, at 262-67.

127. Jayni Foley, Note, *Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases*, 22 BERKELEY TECH. L.J. 447, 458 (2007);

"contents" definition of the Wiretap Act, which is applicable to the SCA, provides that "'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication."[128] Thus, whether information is contents of a communication is generally dependent on whether it is part of the substantive message that a person wishes to communicate or only delivery or processing information.[129]

In some instances, cloud service providers that offer electronic communication or remote computing services to the public are also permitted to disclose the contents of communications.[130] First, obviously, a cloud service provider is permitted to disclose communication contents to an addressee or intended recipient of the communication.[131] Second, the provider may also disclose the contents of a communication with the lawful consent of an addressee or intended recipient.[132] In combination, these two exceptions have an important implication, that is, they make the redirection of a user client to a third party server lawful under the SCA. As shown in Figure 2, (1) if a user enters a cloud service's web address, (2) the requested website will be returned, (3) but in addition the user client is also redirected and discloses information to a third party server, (4) which sends back a frame for display on the requested website. The disclosure of information to the third party server is compliant with the SCA because either the cloud service provider is an addressee or intended recipient of the communication consenting to the disclosure to the third party, or the third party itself is an addressee or intended recipient. Therefore, for example, the redirection of a user client to an ad server is not a disclosure of communication contents under the

Goldberg, *supra* note 119, at 262.

128. 18 U.S.C. § 2510(8).

129. *See, e.g.*, *In re* iPhone Application Litig., 844 F. Supp 2d 1040, 1061 (N.D. Cal. 2012) (citing United States v. Reed, 575 F.3d 900, 916 (9th Cir. 2009)) (holding that contents of communication refers to information the user intended to communicate); Matthew J. Tokson, The *Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2105 (2009) (proposing that information that can reveal the text or subject matter of a communication should be categorized as contents). *See generally* Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 611-16 (2003) (giving an overview on distinguishing content from noncontent in letters, phone calls, emails, and Internet packets).

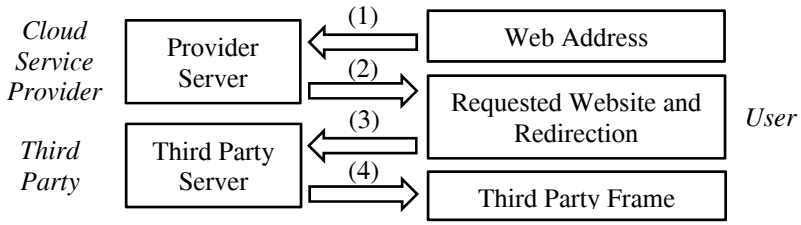
130. *See* 18 U.S.C. § 2702(b).

131. *See id.* § 2702(b)(1).

132. *See id.* § 2702(b)(3).

SCA.[133]

Figure 2. Redirection of a User Client



For a similar reason a user would also have no claim under the Wiretap Act, which prohibits electronic communication service providers from disclosing the "contents of any communication (other than one to such person or entity . . .) . . . to any person or entity other than an addressee or intended recipient of such communication."[134] This is because the communication was either from the user to the cloud service provider, in which case it was a communication "to such person or entity," or from the user to the third party, in which case the third party was an "addressee or intended recipient."[135] In addition, while the redirection of a user client can be a willful interception by the third party and a procurement to intercept by the cloud service provider according to 18 U.S.C. § 2511(1),[136] the interception will be lawful in most cases. Absent a criminal or tortious act, an interception is lawful if performed by a party to the communication or with the consent of one of the parties.[137] In the case

133. *See, e.g., In re* Facebook Privacy Litig., 791 F. Supp. 2d 705, 713-14 (N.D. Cal. 2011) ("Plaintiffs . . . allege that the communications at issue were sent to Defendant or to advertisers. Under either interpretation, Plaintiffs fail to state a claim under the Stored Communications Act.").

134. 18 U.S.C. § 2511(3)(a).

135. *See In re Facebook Privacy Litig.*, 791 F. Supp. 2d at 712-13.

136. *See, e.g.*, United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992) ("[W]hen the contents of a wire communication are captured or redirected in any way, an interception occurs at that time.").

137. § 2511(2)(d); Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001) ("One-party consent is sufficient to negate liability under the consent prong of the Wiretap Act's exception.") (citing United States v. Caceres, 440 U.S. 741, 750 (1979)); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001) ("[W]e find that the DoubleClick-affiliated Web sites are 'parties to the communication[s]' from plaintiffs and have given

of a redirection, either the third party was a party to the communication or the cloud service provider was a party and consented to the redirection.[138] Moreover, it is also required that the alleged interception amounts to a "criminal" or "tortious" act, and in most instances this will not be the case.[139] These terms are construed narrowly, covering only acts accompanied by a specific contemporaneous intention to commit a crime or tort.[140] Particularly, purely commercial purposes are not sufficient for tortious acts and purely commercial intents do not constitute tortious intents.[141]

Beyond the SCA and the Wiretap Act, the disclosure of information to private parties is also subject to various torts. It can satisfy the elements of appropriation of name or likeness,[142] public disclosure of private facts,[143] and false light.[144] However, for the two latter torts, the "highly offensive" requirement reduces the torts' scope of application substantially. Appropriation also has a narrow scope. For example, while it is suggested that collecting and disclosing an extensive consumer profile without consumer consent should be actionable as appropriation,[145] it is not enough to display a consumer's name on a search result page.[146] In addition, cloud service providers are also subject to breach of confidentiality.[147] In this regard, one commentator argues for recognition of a discovery privilege for search queries.[148] Further, a deprivation of use of

sufficient consent to DoubleClick to intercept them." (second alteration in original)).

138. *Chance*, 165 F. Supp. 2d at 1162 (holding that the websites that the user contacted had consented to Avenue A's interception of the communication between them and the user).

139. *See* § 2511(2)(d).

140. *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 515.

141. *See id.* (concluding that defendant's commercial motivations negate tortious intent).

142. *See* RESTATEMENT (SECOND) OF TORTS § 652C (1977); Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 803-810 (N.D. Cal. 2011) (denying Facebook's motion to dismiss a claim of commercial misappropriation under California Civil Code Section 3344).

143. *See* RESTATEMENT (SECOND) OF TORTS § 652D (1977).

144. *See id.* § 652E.

145. Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 69 (2003).

146. Stayart v. Google Inc., 783 F.Supp.2d 1055, 1057 (E.D. Wis. 2011).

147. *See* Tene, *supra* note 54, at 1486-90 (arguing that search engine providers are subject to the law of confidentiality). *See generally* SOLOVE & SCHWARTZ, *supra* note 24, at 73 (comparing the torts of public disclosure of private facts and breach of confidentiality); Susan M. Gilles, *Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy*, 43 BUFF. L. REV. 1 (1995) (discussing whether breach of confidence is an effective instrument for privacy protection).

148. *See* Werner, *supra* note 119, at 274.

personal information for a substantial period of time is arguably actionable as trespass to chattels.[149] However, the disclosure or transfer of information alone does not constitute a remediable harm and even if such harm exists, it rarely amounts to a diminishment of the quality or value of a materially valuable interest in personal information.[150]

In certain areas cloud service providers have to adhere to special disclosure requirements. For example, cloud service providers that offer "video cassette tapes or similar audio visual materials" are arguably subject to the Video Privacy Protection Act, which generally prevents them from knowingly disclosing PII concerning their customers.[151] This obligation is especially relevant as it also extends beyond the immediate providers of audio visual materials.[152] For book service providers, California's Reader Privacy Act limits the disclosure of a user's personal information as well.[153] However, information can be disclosed if the user has given "informed, affirmative consent to the specific disclosure for a particular purpose."[154] If health care providers and other covered entities under the Health Insurance Portability and Accountability Act (HIPAA) provide cloud services, they will be often limited in disclosing and using patients' information.[155] The same is also true for financial information collected by financial institutions or other processors of financial information.[156]

2. Disclosure to the Government

The disclosure of user information to the government is contingent on the user's constitutional privacy rights, particularly, the

149. *See In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 328-29 (E.D.N.Y. 2005).

150. *Id.*

151. *See* 18 U.S.C. § 2710 (2011); Class Action Complaint at 46, Lane v. Facebook, Inc., 696 F.3d 811 (9th Cir. 2012) (No. C08 03845 RS), 2008 WL 3886402, para. 131.

152. *See* § 2710(a)(4), (b)(2)(D)-(E) (2011).

153. *See* CAL. CIV. CODE §§ 1798.90-1798.90.05 (West 2012).

154. *See id.* § 1798.90(c)(3).

155. *See* 45 C.F.R. § 164.502-.514 (2012). Beyond HIPAA further federal and state statutes govern the disclosure of health information. *See, e.g.*, 42 U.S.C. § 290dd-2 (2011).

156. *See, e.g.*, Gramm-Leach-Bliley Act of 1999, Pub. L. 106-102, 113 Stat. 1338 (relevant sections codified as amended in 15 U.S.C. §§ 6801-6809 (2011)), and the implementation of its Privacy Rule and Safeguards Rule, in 16 C.F.R. pts. 313 and 314 (2012), respectively.

Fourth Amendment and possibly the right to information privacy. Beginning with the Fourth Amendment, whether its protection from governmental searches and seizures is applicable depends on the "reasonable expectations of privacy" test of *Katz v. United States*.[157] In the context of cloud computing, the reasonable expectation of privacy is limited by the third-party doctrine.[158] This doctrine was developed in *United States v. Miller*, where the Supreme Court reasoned that voluntary revelation of information to a third party can justify an assumption of risk that the third party will disclose the revealed information to the government, which would counter a reasonable expectation of privacy.[159] However, a reasonable expectation of privacy can still exist in cases where contents of a communication are revealed to a third party. *Smith v. Maryland* stands for the proposition that Fourth Amendment protection can continue to apply with regard to the contents of a communication because in this case a reasonable expectation of privacy is more likely to exist than for noncontent information.[160] While this distinction between contents of communication and noncontent information is subject to criticism,[161] it remains an essential element of Fourth Amendment doctrine.[162]

---

157. *See* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring). *See also* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 215 (1890) ("There are persons who may *reasonably claim* as a right, protection from the notoriety entailed by being made the victims of journalistic enterprise." (emphasis added)).

158. *See, e.g.*, Constantine, *supra* note 109, at 513; Kattan, *supra* note 123, at 625; Robison, *supra* note 123, at 1226; Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1135 (2002).

159. *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities . . . ."). *See also* Smith v. Maryland, 442 U.S. 735, 743-44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

160. *See Smith*, 442 U.S. at 741 ("Yet a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications.").

161. *See, e.g.*, *Smith*, 442 U.S. at 748 (Stewart, J., dissenting) (doubting that there is a clear distinction between content and noncontent); David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2237 (2009) ("But while calendars, photo albums, and the like are more clearly content data as opposed to transactional, other types of data are less clear.").

162. *See, e.g.*, Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1029 (2010) ("The Fourth Amendment should generally protect the contents of communications stored in 'the cloud' of the Internet . . . ."); Tene, *supra* note 54, at 1471 ("Hence, Fourth Amendment protection continues to apply insofar as personally identifiable information held by a third party includes the 'contents' of a

Because of the third party doctrine, a cloud service user may only have a limited expectation of privacy in certain instances.[163] For example, a user may be held to have relinquished a reasonable expectation of privacy in search queries upon submitting them to the search engine provider.[164] In such case the user is deemed to have voluntarily turned over information to a third party and is therefore only entitled to limited Fourth Amendment protection.[165] Only to the extent that search queries and other collected information can be characterized as contents of a communication, constitutional protection can be reasserted under the *Smith* exception.[166] In this regard, for instance, the body of an email message qualifies as communication contents.[167] In general, in order to determine the scope of protection for a particular piece of information, it must be determined whether that piece of information is contents of a communication or noncontent information. As described for the SCA and Wiretap Act, information is contents of a communication if it is part of a substantive message that a person wishes to communicate, while delivery or processing information will usually not be considered contents of a communication.[168]

In addition to the Fourth Amendment, to a limited extent, cloud service providers could be subject to a right to information privacy as well. The Supreme Court mentioned the right to information privacy in *Whalen v. Roe*.[169] It is not clear, however, whether the Constitution

---

communication.").

163. *See* United States v. Forrester, 512 F.3d 500, 512 (9th Cir. 2008) (holding that email and IP addresses do not receive Fourth Amendment protection); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (concluding that users cannot have a reasonable expectation of privacy in bulletin board subscriber information); Foley, *supra* note 127, at 457.

164. Tene, *supra* note 54, at 1472.

165. *Id.*

166. *Id.*

167. *See* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) ("It follows that email requires strong protection under the Fourth Amendment . . . ."); *Forrester*, 512 F.3d at 512 (holding that the contents of emails may receive Fourth Amendment protection); Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007) (holding that "individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial [Internet service provider]"), *vacated en banc*, No. 06-4092, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 9, 2007); United States v. Maxwell, 45 M.J. 406, 417-19 (C.A.A.F. 1996) (holding that emails may be protected under the Fourth Amendment).

168. *See supra* Part III.B.1.

169. *See* Whalen v. Roe, 429 U.S. 589, 598-99 (1977) (acknowledging an "individual interest in avoiding disclosure of personal matters"). *See also* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 465 (1977) (holding that President Nixon "has a legitimate expectation of privacy

can be interpreted to contain such right. While some courts held so,[170] others expressed doubts.[171] In a recent decision, the Supreme Court avoided to take a stand.[172] Assuming that the right can be derived from the Constitution, it would protect the "individual interest in avoiding disclosure of personal matters."[173] This protection could become especially relevant as the third party doctrine is arguably not applicable to the right to information privacy.[174] However, the right only protects from "hav[ing] an individual's private affairs made public *by the government*."[175] Thus, it only applies to governmental cloud service providers or to private providers if they act as an agent of the government.[176] Given the existence and applicability of the

in his personal communications"); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980) (establishing a seven factor test for determining whether the right to information privacy is violated).

170. *See, e.g.*, *In re* Crawford, 194 F.3d 954, 959 (9th Cir. 1999) (stating that the right to informational privacy is not absolute, but rather to be weighed with governmental interests) (quoting Doe v. Att'y Gen., 941 F.2d 780, 796 (9th Cir. 1991)); *Westinghouse Elec. Corp.*, 638 F.2d at 578. *See also* Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 BRANDEIS L.J. 643, 653 (2007) (stating that "there is a strong argument that the Constitution should be interpreted to protect a right to control information").

171. *See, e.g.*, Am. Fed'n of Gov't Emps. v. Dep't of Hous. & Urban Dev., 118 F.3d 786, 793 (D.C. Cir. 1997) (refraining from ruling whether a right to information privacy exists); J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981) (concluding that the Federal Constitution does not encompass a general right to nondisclosure of private information). *See also* Strahilevitz, *supra* note 93, at 2048 (arguing that "it would be best to end the constitutional right to information privacy experiment" or relegate it to a gap-filling function).

172. Nat'l Aeronautics & Space Admin. v. Nelson, 131 S. Ct. 746, 751 (2011) ("We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*.").

173. *Nixon*, 433 U.S. at 457 (quoting *Whalen*, 429 U.S. at 599); *Whalen*, 429 U.S. at 599-600; *Westinghouse Elec. Corp.*, 638 F.2d at 578 (citing *Whalen*, 429 U.S. at 599-600).

174. Nelson v. Nat'l Aeronautics & Space Admin. (*Nelson II*), 568 F.3d 1028, 1031 n.7 (9th Cir. 2009) (Wardlaw, J., concurring) (citing Nelson v. Nat'l Aeronautics & Space Admin. (*Nelson I*), 530 F.3d 865, 880 n.5 (9th Cir. 2008), *rev'd and remanded*, 131 S. Ct. 746 (2011)), *rev'd and remanded*, 131 S. Ct. 746 (2011); *Nelson I*, 530 F.3d at 880 n.5. *But see Nelson II*, 568 F.3d at 1044 (Callahan, J., dissenting) (arguing that the interpretation of the right to informational privacy is "informed by Supreme Court case law interpreting an expectation of privacy under the Fourth Amendment"); Strahilevitz, *supra* note 93, at 2043 (arguing in favor of Judge Callahan's dissent).

175. *Westinghouse Elec. Corp.*, 638 F.2d at 577 (emphasis added). *See also Nelson I*, 530 F.3d at 877 (stating that the "*government's actions* [that] compel disclosure of private information" must advance a legitimate state interest and be narrowly tailored to be justified (emphasis added)).

176. For a private person to be considered an agent of the government under the state action doctrine, two factors are determinative: (1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the private actor's purpose was to assist law enforcement efforts rather than to further its own ends. *See, e.g.*, United States v. Steiger, 318

right to information privacy, the lawfulness of the information disclosure would depend on the seven-factor test established by *United States v. Westinghouse*.[177]

In contrast to the Federal Constitution, many state constitutions protect privacy in the form of a right to information privacy unequivocally.[178] One example is the right to information privacy found in the California Constitution.[179] Going beyond the Federal Constitution's information privacy right interpretation, California's constitutional privacy right "protects individuals from the invasion of their privacy not only by state actors, but also by private parties."[180] Thus, the Californian information privacy right's applicability is broader than the possible right under the Federal Constitution. However, its scope of privacy protection is actually smaller. This is because in order to prove a claim under California's constitutional privacy right, a plaintiff must demonstrate three elements: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; (3) and conduct by the defendant that amounts to a serious invasion of the protected privacy interest,"

F.3d 1039, 1045 (11th Cir. 2003) (citing United States v. Simpson, 904 F.2d 607, 610 (11th Cir. 1990)). *See also* Volokh, *supra* note 6, at 85 ("The Constitution says little about what private persons or businesses may or may not do . . . .").

177. *Westinghouse Elec. Corp.*, 638 F.2d at 578 (holding that the right to information privacy is dependent (1) on the type of record requested; (2) the information it does or might contain; (3) the potential for harm in any subsequent nonconsensual disclosure; (4) the injury from disclosure to the relationship in which the record was generated; (5) the adequacy of safeguards to prevent unauthorized disclosure; (6) the degree of need for access; and (7) whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access).

178. *See, e.g.*, Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 654 (Cal. 1994) (en banc) (holding that the privacy provision of the California Constitution encompasses informational privacy); Berkeley v. Eisen, 699 So. 2d 789, 791 (Fla. Dist. Ct. App. 1997) (holding that the names, addresses, and phone numbers of investors were protected from public disclosure under Florida's constitutional privacy right); McCloskey v. Honolulu Police Dep't, 799 P.2d 953, 957 (Haw. 1990) (holding that Hawaii's constitutional right of privacy protects the individual's interest in avoiding disclosure of personal matters); State v. Nelson, 941 P.2d 441, 448 (Mont. 1997) (holding that Montana's constitutional privacy right encompasses informational privacy). For a comprehensive overview of explicit state constitutional privacy protections see *Privacy Protections in State Constitutions*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/privacy-protections-in-state-constitutions.aspx (last visited Mar. 21, 2013).

179. CAL. CONST. art. I, § 1.

180. *See, e.g.*, Leonel v. Am. Airlines, Inc., 400 F.3d 702, 711-12 (9th Cir. 2005); *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (citing Am. Acad. of Pediatrics v. Lungren, 940 P.2d 797 (Cal. 1997)); Huntingdon Life Scis., Inc. v. Stop Huntingdon Animal Cruelty USA, Inc., 29 Cal. Rptr. 3d 521, 546 (Ct. App. 2005).

that is, an egregious breach of the social norms underlying the privacy right.[181] In particular, the third element will often limit the scope of privacy protection of cloud service users. For example, the disclosure of unique device identifier numbers, personal information, and location information does not amount to an egregious breach of social norms.[182]

Below the constitutional level, the disclosure of information to the government is generally regulated by the same laws as the disclosure to private parties.[183] Some laws, however, already reflect the Fourth Amendment's privacy protection by providing special rules for the disclosure of information to the government.[184] For example, the provisions of the SCA implement the Fourth Amendment.[185] Specifically, 18 U.S.C. § 2703 regulates compelled information disclosure by electronic communication and remote computing service providers. In this regard, every compelled information disclosure is an information disclosure to the government.[186] Reflecting the Fourth Amendment jurisprudence, 18 U.S.C. § 2703 distinguishes between disclosure of contents of communication and noncontent information. On the one hand, the compelled disclosure of contents of communications is subject to strict requirements. Specifically, such disclosure can be based on a

181. *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1063 (citing *Hill*, 865 P.2d at 654-55).

182. *Id.*

183. *See supra* Part III.B.1.

184. *See, e.g.*, 18 U.S.C. §§ 2703, 2710(b)(2)(C), 2710(b)(3) (2011). *See also* CAL. CIV. CODE § 1798.90(c)(1)-(2) (West 2012). All laws must be construed in light of the constitutional privacy rights, independently of whether those rights are already explicitly reflected in the language of the laws or not. *See, e.g.*, Cutter v. Brownbridge, 228 Cal. Rptr. 545, 550 (Ct. App. 1986) (holding that "[a]ny incursion into the protected interest should be construed, if possible, to preserve the privacy interest, and so that the statute is not applied in an unconstitutional manner").

185. *See* Andrew C. DeVore, *Cloud Computing: Privacy Storm on the Horizon?*, 20 ALB. L.J. SCI. & TECH. 365, 371 (2010) (explaining that Congress passed the Electronic Communications Privacy Act "to approximate Fourth Amendment and other protections for electronic communications and other information stored electronically"); Kerr, *supra* note 83, at 1212 (noting that the statute creates a set of Fourth Amendment-like privacy protections). *But see* Tene, *supra* note 54, at 1481 (arguing that the Fourth Amendment's reasonable expectation of privacy test is only insufficiently reflected in 18 U.S.C. § 2703).

186. However, not every information disclosure to the government may be a compelled information disclosure. In this regard, it is a difficult task to draw the distinction between compelled and voluntary information disclosure. *See* Kerr, *supra* note 83, at 1224-27.

warrant,[187] which, in case of disclosure by an electronic communication service provider of information in storage for one hundred and eighty days or less, is even required,[188] a subpoena combined with prior notice to the subscriber or customer,[189] or a court order combined with such notice.[190] On the other hand, noncontent information is less protected by the Fourth Amendment and, consequently, subject to less strict disclosure requirements.[191]

C. Information Use

Information use covers the various ways of aggregating and analyzing information for a particular purpose. Information aggregation and analysis can serve many different purposes. Relevant purposes for cloud service providers are, for example, provision, maintenance, and improvement of services and advertisements. In order to analyze the information, providers can leverage computer scientific methods, such as data mining, as well as statistical and mathematical methods.[192] Information aggregation, in form of online profiling or data enhancement, is often a prerequisite for the analysis of information and is mainly governed by unfair competition laws. The remainder of this section will address information aggregation.

Information aggregation is the process of connecting information.[193] While it is based on the collection of information, it goes further because it systematically connects information. For example, an aggregation can refer to all information associated with a particular user of a cloud service. Thus, aggregated information can be used for purposes of personalization of cloud services or behavioral advertising.[194] For services that do not require users to authenticate themselves, information can be aggregated based on IP

187. 18 U.S.C. § 2703(a), (b)(1)(A) (2011).

188. *Id.* § 2703(a).

189. *Id.* § 2703(b)(1)(B)(i).

190. *Id.* § 2703(b)(1)(B)(ii), (d).

191. *Id.* § 2703(c).

192. *See* Tene, *supra* note 54, at 1450-51 (noting that search engine providers can refine search quality and build new services by analyzing search query logs).

193. *See* Solove, *supra* note 74, at 490 ("*Aggregation* involves the combination of various pieces of data about a person.").

194. Eve Chaurand-Fraser, *Current Events in Search Data Collection and Retention*, 970 PLI/PAT 609, 612 (2009). *See generally* Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149, 1186-88 (2008) (describing search engine personalization).

addresses or cookie IDs, which are identifiers that can be associated with particular computers or browsers, respectively.[195]

The lawfulness of information aggregation depends on whether it is limited to information that the cloud service provider collected itself or involves information collected via third parties. If the cloud service provider only aggregates information that it collected itself, such practice is generally permitted without user consent.[196] The FTC published guidelines for aggregating consumer information.[197] According to those guidelines, the aggregation of information from consumer-to-business transfers of information generally does not require consent by the consumer.[198] However, a cloud service provider may need to obtain consent when tracking a consumer across multiple of its services.[199]

If any information to be aggregated is collected via third parties, consent will often be required. This is especially true for third party tracking, that is, following a consumer across third party websites.[200] In case of a business-to-business transfer of consumer information, it must be distinguished between receiving and disclosing information.[201] If a cloud service provider receives consumer information in order to aggregate it with information it already collected itself, the FTC does not require consent of the consumer.[202] However, if a cloud service provider with a direct consumer relationship discloses information to a third party, the consent of the consumer is required.[203]

D. Information Management

Information management refers to the maintenance of information and is primarily governed by unfair competition laws. In

195. Goldberg, *supra* note 119, at 253.

196. *Cf.* Tracy A. Steindel, Note, *A Path Toward User Control of Online Profiling*, 17 MICH. TELECOMM. & TECH. L. REV. 459, 460 (2011) ("Congress has not passed any relevant legislation, and courts have proven unwilling to read existing legislation to prohibit or limit online profiling."). *See generally In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

197. *See* FED. TRADE COMM'N, *supra* note 68, at 42-46.

198. *Id.* at 44.

199. *Id.* at 41-42.

200. *Id.* at 40-41.

201. *Id.* at 44.

202. *Id.*

203. *Id.*

this regard, the FTC requires cloud service providers to develop and implement a comprehensive privacy and security program subject to an independent third party audit.[204] Thus, the remainder of this section will focus on the details of such program, that is, providers' obligations to develop and implement measures for controlling access to information as well as for retention, disposal, storage, and transmission of information. Furthermore, the extensive state legislation in the area of information breach notification will be addressed as well.

With regard to controlling information access, cloud service providers are required to employ reasonable and appropriate measures to protect personal information against unauthorized access.[205] This involves employing an intrusion detection system, monitoring system logs, restricting connections to specified IP addresses or granting temporary, limited access, monitoring and filtering outbound traffic from the provider's networks to identify, and block export of sensitive information without authorization.[206] Cloud service providers are also required to develop reasonable policies and procedures to verify or authenticate the identities and qualifications of users and identify unauthorized user activity.[207]

There is no fixed retention period for information. The FTC, however, charged various companies under the FTC Act for retaining credit card information longer than they had a business need to do so.[208] Thus, service providers must generally dispose of information if there is no longer a business need to retain it.[209] This remains true

204. *See, e.g.*, Decision and Order at 5-7, Facebook, Inc., FTC Docket No. C-4365 (July 27, 2012); Decision and Order at 4-5, Google, Inc., FTC Docket No. C-4336 (Oct. 13, 2011).

205. *See, e.g.*, Decision and Order at 3, CVS Caremark Corp., FTC Docket No. C-4259 (June 18, 2009); Complaint for Injunctive and Other Equitable Relief at 18-19, FTC v. Wyndham Worldwide Corp., Civ. No. 2:12-cv-01365-SPL, 2012 WL 2389423 (D. Ariz. June 26, 2012); Complaint at 3-5, Franklin's Budget Car Sales, Inc., FTC Docket No. C-4371 (Oct. 3, 2012) (alleging misrepresentations about the implementation of reasonable and appropriate measures to protect consumers' personal information from unauthorized access as well as violations of the Gramm-Leach-Bliley Act's Safeguards Rule, 16 C.F.R. pt. 314, and Privacy Rule, 16 C.F.R. pt. 313, which were applicable to the respondent as it was characterized as a financial institution).

206. Complaint at 2, Dave & Buster's, Inc., FTC Docket No. C-4291 (May 20, 2010).

207. Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 6-9, United States v. ChoicePoint Inc., No. 1:06-CV-00198-GET (N.D. Ga. Jan. 30, 2006).

208. *See, e.g.*, Decision and Order at 2, DSW Inc., FTC Docket No. C-4157 (Mar. 7, 2006); Complaint at 2-3, BJ's Wholesale Club, Inc., FTC Docket No. C-4148 (Sept. 20, 2005).

209. *See also* 16 C.F.R. § 312.10 (2012) (prescribing that personal information collected

even if laws provide for disclosure of information to the government. For example, while the SCA provides that the government can compel disclosure of certain information for a potentially infinite time,[210] the service provider is not obligated to retain information for the government beyond its business purposes. Rather, it is the responsibility of the government to make a request early enough, when the information is still retained for business purposes. Upon such request, however, it is the provider's obligation to preserve the pertinent information for the government.[211]

When it is no longer necessary to retain information, cloud service providers must dispose of the information in a manner that preserves privacy.[212] Many states have statutes that require covered cloud service providers to dispose of personal information safely and securely.[213] For example, California requires businesses to take reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (1) shredding, (2) erasing, or (3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.[214]

In certain cases, cloud service providers must have encryption for storage and transmission of information.[215] Particularly, it is insufficient to store debit and credit card information in unencrypted files that could be easily accessed by using a commonly known user ID and password.[216] Further, it is unlawful to transmit debit and credit card information, financial account numbers, security codes and

---

online from a child should only be retained "as long as is reasonably necessary to fulfill the purpose for which the information was collected.").

210. 18 U.S.C. §§ 2703(a)-(b) (2011).

211. *Id.* § 2703(f).

212. *See, e.g.*, Decision and Order at 2, CVS Caremark Corp., FTC Docket No. C-4259 (June 18, 2009); Complaint at 2-3, Rite Aid Corp., FTC Docket No. C-4308 (Nov. 12, 2010).

213. For a comprehensive overview of state information disposal statutes, see SOLOVE & SCHWARTZ, *supra* note 24, at 142-43. In addition, the Disposal Rule, 16 C.F.R. § 682 (2011), is applicable to cloud service providers that hold information from consumer reports.

214. CAL. CIV. CODE § 1798.81 (West 2012).

215. *See, e.g.*, Complaint at 2-3, DSW Inc., FTC Docket No. C-4157 (Mar. 7, 2006); Complaint at 2-3, BJ's Wholesale Club, Inc., FTC Docket No. C-4148 (Sept. 20, 2005)**.** Some state laws require the encryption of information in certain cases as well. *See, e.g.*, NEV. REV. STAT. § 603A.215(2), (5) (2011), 201 MASS. CODE REGS. § 17.04(3), (5) (2013).

216. Complaint at 2, DSW Inc., FTC Docket No. C-4157; Complaint at 2-3, BJ's Wholesale Club, Inc., FTC Docket No. C-4148.

expiration dates, and Social Security numbers entered into web forms over the Internet unencrypted and in clear text.[217] In some instances, the FTC even required to encrypt or otherwise protect user credentials, search queries, and search results in transit between users and cloud service providers.[218]

If a data security breach happens, cloud service providers must notify affected users.[219]A large majority of states have data security breach notification statutes.[220] Some of these statutes have subtle and noteworthy differences. For example, California's data security breach notification statute requires the disclosure of any actual or reasonably suspected security breach concerning unencrypted personal information.[221] However, New York's data security breach notification statute can cover encrypted data as well if an encryption key has also been acquired.[222] If cloud service providers want to avoid multi-state notifications, they could alternatively adhere to the strictest state statute, which will act as a de facto federal standard.

IV. CONCLUDING REMARKS

Cloud computing is not a new phenomenon and covers many web applications and other network services that already existed before the term "cloud computing" was coined. In fact, even before the trend of moving software and information to the desktop emerged in the 1990s, many information processing tasks were performed via the cloud.[223] Therefore, a lot of the legal considerations, for example, the various applications of the SCA, are not new either. While not a perfect fit in every detail, on a structural level the privacy law of

217. Complaint at 3, Upromise, Inc., FTC Docket No. C-4351 (Mar. 27, 2012).

218. Complaint at 4, Reed Elsevier Inc., FTC Docket No. C-4226 (July 29, 2008).

219. *See generally* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007). *See also* CAL. CIV. CODE § 1798.83 (California's "Shine the Light" law, which requires businesses to notify customers about the disclosure of personal information to third parties independently of any data security breach).

220. For a comprehensive overview of data security breach notification statutes see SOLOVE & SCHWARTZ, *supra* note 24, at 136-40.

221. CAL. CIV. CODE § 1798.82(a).

222. N.Y. GEN. BUS. LAW § 899-aa(b) (McKinney 2012).

223. *See, e.g.*, Armbrust et al., *supra* note 2, at 50 (quoting Oracle's CEO Larry Ellison, with the statement that "[t]he interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do . . . . I don't understand what we would do differently in the light of cloud computing other than change the wording of some of our ads." (alteration in original)).

cloud computing can be soundly and coherently interpreted. Most importantly, it is characterized first by the autonomy of the service providers and users entering into privacy contracts and secondly by a set of secondary privacy laws as a default. As it should be, the law is guided by "autonomous individuals who are able to negotiate freely and equally for the right level of privacy."[224]

Based on these characteristics the law allows for development of a privacy marketplace, where both the personal and commercial dimensions of the privacy right can be individually adapted.[225] For example, in exchange for free services, users can authorize service providers to collect, disclose, and use their information for contextual and targeted advertising.[226] In this regard, it is left to the users how strongly they want to monetize their privacy rights and how much privacy they want to retain. On the other side, cloud service providers are enabled to offer new services and generate revenue from the information they collect.[227] They can obtain rights in information uploaded to the cloud in exchange for providing access to free-of-charge services.[228] In this regard, the privacy law of cloud computing promotes free markets and innovation serving as a blueprint for the American information privacy regime.

224. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1682 (1999).

225. *See generally* Christopher Riederer et al., *For Sale: Your Data, By: You*, *in* HOTNETS-X PROCEEDINGS OF THE 10TH ACM WORKSHOP ON HOT TOPICS IN NETWORKS 1 (2011), *available at* http://conferences.sigcomm.org/hotnets/2011/papers/hotnetsX-final85.pdf.

226. Robison, *supra* note 123, at 1196.

227. Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 641 (2008).

228. Gervais & Hyndman, *supra* note 29, at 78.