The Problem of Onward Transfers under U.S. Law

Raghu Seshadri
Attorney, Wilson Sonsini Goodrich & Rosati
650 Page Mill Road
Palo Alto, CA 94304-1050
rseshadri@wsgr.com

Abstract
Several of the major U.S. federal and state laws regulating the collection, use and disclosure of personal information by business entities only regulate the activities of entities that receive personal information directly from consumers while ignoring third-parties that receive this personal information through onward transfers. This regulatory gap opens the door for such third parties to use or disclose personal information that they receive from regulated entities in derogation of such regulated entities’ stated policies without risk of government interference.

Issue Summary
In its report on fair information practice principles the FTC stated that “it is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them.” While the FTC is seeming to state the obvious, many of the laws regulating the information privacy practices of business entities in the United States are only enforceable against the party collecting personal information directly from the consumer while ignoring third parties who receive personal information via onward transfer. This Issue Paper will summarize portions of several key statutes to highlight this regulatory gap, and will describe some possible solutions.

FTC Act
Under the FTC Act unfair or deceptive acts or practices in or affecting commerce are declared unlawful, and the FTC is given the power to prevent such practices. The FTC has used this power to initiate actions against several entities for failing to comply with such entities’ posted privacy statements. However, the FTC has not used this power to regulate the activities of those third parties who obtain personal information through onward transfers, and who either receive such information in derogation of the collecting party’s policies, or use or disclose such information in derogation of the collecting party’s policies. It is unclear whether the FTC would consider such actions unfair or deceptive acts or practices.

Children’s Online Privacy Protection Act (“COPPA”)
COPPA only applies to an “operator of a web site or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child.” An “operator” is a person who operates a website or an online service and collects or maintains personal information from or about the users of the website or online service. COPPA imposes notice and parental consent requirements surrounding the collection, use, and disclosure of personal information from children under 13.

Since COPPA does not regulate the actions of third parties that do not operate web sites directed toward children (e.g. data brokers) and who receive children’s personal information from a COPPA-regulated entity rather than “from a child”, such third parties could potentially use or disclose a child’s personal information without regard to parental consent or risk of interference by the federal government.

State Statutes
Minnesota and Nevada both only prohibit internet service providers (rather than all entities collecting information over the internet) from disclosing certain customer information without opt-in consent. California and Utah both require non-financial businesses to disclose to their consumers the types of personal information they share with third parties for direct marketing purposes or compensation respectively. California also requires all operators of commercial web sites or online

---

1 http://www.ftc.gov/reports/privacy3/fairinfo.shtm
3 See http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html
4 15 USC § 6502(a).
7 See Minnesota Statutes §§ 325M.01 to .09; Nevada Revised Statutes § 205.498
services that collect personally identifiable information about individual California consumers who visit the service or website to post a privacy policy describing the categories of personally identifiable information that are collected. Similar to the FTC Act, both Nebraska and Pennsylvania prohibit false or misleading statements in privacy policies. What these statutes all have in common is that they regulate the activities of the party collecting personal information rather than the third parties receiving the information through an onward transfer, again resulting in a regulatory gap.

The E.U. Safe Harbor
The U.S. Department of Commerce, in conjunction with the European Commission, has developed a safe harbor framework under which U.S. companies can certify that they provide "adequate" privacy protections sufficient to permit a transfer of data under the E.U. Data Protection Directive (95/46/EC) (the "Directive") by adhering to certain principles. One of these principles, "Onward Transfer", requires certifying organizations to apply Notice and Choice principles before disclosing information to third parties. In addition, where a certifying organization wishes to transfer information to a third party acting as an agent, it must either ascertain that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles. While the Directive itself directly regulates third-party data processors and thereby ensures consistent treatment of transferred information within the E.U., the safe harbor only applies to the certifying organization, and (with the exception of third parties acting as "agents") does not require the certifying entity to impose any controls on third parties obtaining information from a certifying entity.

Conclusions
Several of the mechanisms which are designed to protect consumer personal information from unauthorized collection, use and disclosure in the United States fail to adequately protect such information since they do not regulate the third parties obtaining personal information through onward transfers.

Potential Solutions

Contractual Regulation
It may be argued that by imposing liability on the party collecting information, third parties are indirectly regulated since the collecting entity is incentivized to impose contractual restrictions on third parties to whom they provide personal information. However, this argument presents several potential shortfalls. First, even if contractual restrictions are imposed, it is not clear that the collecting party will have the resources to adequately police the third party’s actions. Second, the language of the applicable contract may not incentivize the third party to impose the same downstream restrictions on those parties to which it provides information. Finally, it is not clear that the issue of data use and disclosure is actually addressed in these agreements in practice.

Amending Existing Laws
Another possible solution is to amend the inadequate laws and regulations so that they address the activities of third parties directly as is already the case with respect to the Health Insurance Portability and Accountability Act ("HIPAA") and the Gramm-Leach-Bliley Act ("GLBA"). While this solution might work with respect to those specific categories of information targeted by U.S. sectoral laws (e.g. nonpublic personal information under the GLBA, protected health information under HIPAA, information collected from children under COPPA), this approach would not result in comprehensive regulation of all types of personal information collected by business entities via onward transfers. Specifically, it seems that any broad-based application would require implementation of the FTC’s power to police unfair or deceptive acts or practices, and so far the FTC has not indicated that a third party’s use or disclosure of personal information in derogation of the collecting party’s privacy policy constitutes an unfair or deceptive act or practice.

Comprehensive Reform
Comprehensive privacy reform may present another solution. Specifically new law(s) covering a broad range of personal information and imposing restrictions on all commercial entities’ collection, use, and disclosure of this personal information could fill the regulatory gap in the United States. However, passage of such broad-based reform would require a fundamental shift from the existing regulatory model and consequently may not be realistic.

---

10 See Nebraska Stat. § 87-302(14); 18 Pa. C.S.A. § 4107(a)(10).
11 See http://www.export.gov/safeharbor/eg_main_018236.asp
12 See http://www.export.gov/safeharbor/eu/eg_main_018475.asp
13 See id.
14 As a result of the American Recovery and Reinvestment Act of 2009, “business associates” will be directly regulated by HIPAA starting in February 2010. “Business associates” include many of the third parties to whom a covered entity supplies information. In addition, the GLBA directly regulates reuse of information by nonaffiliated third parties that receive nonpublic personal information from a financial institution. See 15 U.S.C. § 6802(c)
References
15 U.S.C. §§ 41, 45, 46, 57a, 57b, 57b-1, as amended
15 U.S.C. §§ 6501-6505, as amended
45 C.F.R. 164
Minnesota Statutes §§ 325M.01 to .09
Nevada Revised Statutes § 205.498
Cal. Civil Code §§ 1798.83 to .84
Utah Code §§ 13-37-101-102, and 201-203
Cal. Bus. & Prof. Code § 22575
Nebraska Stat. § 87-302(14)
18 Pa. C.S.A. § 4107(a)(10)
http://www.ftc.gov
http://www.export.gov