



Jun 18, 2015

Categories:

[Blockchain and Digital](#)

[Assets](#)

[Blogs](#)

[Publications](#)

Developments in the Rules Governing Personal Identifiable Information May Have Unexpected Consequences for Lenders And Other Businesses.

In February [?of 2015?], one of the original and legendary tech chains, RadioShack (RS), filed for Chapter 11 bankruptcy. (For years RS labeled itself as “America’s technology store”. In 1977, RS introduced the TRS-80, one of the first personal computers). As a result, PII collected by RS over many years along with a number of its other assets, was almost sold by a bankruptcy trustee to a third party to help pay off Radio Shack’s debts.

For years, RS had collected email addresses, telephone numbers and other PII from customers. (Remember Kramer asking, “Why does Radio Shack ask for your phone number when you buy batteries?” Answer: “I don’t know.”).

Indeed, RS pioneered the collection of PII data. And by the time it filed bankruptcy RS had dutifully collected over 13 million email addresses and 65 million customer names and physical addresses, as well as information about some 117 million customers’ shopping habits.

RS had a privacy policy that would seem to have prevented such a sale to a third party. RS’s policy went so far as to commit not to sell the information and that it would provide the information to others only when the customers consented, or when required to do so by law. (The company did reserve the right to change its policies at any time.)

In a last-minute revision to its offer, the purchaser of the RS assets agreed that customer data would not be part of the sale. The planned inclusion of PII had prompted objections from government authorities in several states.

Nevertheless, there was significant speculation in the media and the tech world over the propriety of the sale of the PII collected by RS

and whether there were ample safeguards in place. Indeed, the proposed transaction raised interesting privacy issues; such PII sales pit the privacy interests of customers and the public against the interests and freedom of a business owner or even a bankruptcy trustee to sell assets of a company. And the proposed transaction also raised inquiries as to the freedom of a purchaser of assets to use the assets it paid for in ways that may not be consistent with the seller's privacy policy.

Is a privacy policy a contractual commitment or is it just a policy of the company that can be ignored or altered? Is it mere puffery? Can consumers challenge such sales? Can the Federal Trade Commission (FTC)? By looking at three different situations, the answers perhaps become a little clearer.

On one end of the spectrum lies the company who wishes to sell collected PII and its privacy policy reflects both this possibility and the consent of its customers. Since there are no overarching federal statutes providing privacy protection and state laws generally are more specific to practices rather than data protection, this company may be free to sell such information, consistent with its policy.

A key issue, however, is whether the customers can be said to have knowingly "consented." Indeed, whether consent was validly, freely and knowingly given can often create litigation issues. See for example *Kirch v Embarq Management Co.*, 2011 WL 3651359 (D. Kan. ,2011), *Deering v. CenturyTel Inc.* 2011 WL 1842859 (D. Mont. 2011), *In re Google Inc. Gmail Litigation* 2014 WL 1102660 (N.D.Cal. 2014). The FTC requires that there be clear and conspicuous notice and affirmative consent.

In any event, assuming the policy permits the sale, consumers would be hard pressed to show damages as a result of the sale (i. e., they have no standing) and absent the violation of some specialized regulations or statutes (such as GLBA, HIPAA or credit card protection statutes and regulations), there is little that could be challenged. Again, FTC requirements for customer consent must be met.

Thorny issues arise, however, in the more common situation when the seller decides to sell PII arguably in a manner not consistent with its policy, where customers have not clearly consented or the purchaser decides not to follow the policy once the transaction is completed.

First, some states, such as Texas and Tennessee, actually specifically prohibit companies from selling PII in ways that violate the company's own privacy policies. (In the RadioShack case, 24 states legally challenged the PII sale.)

Moreover, the FTC has determined that the sale or assignment of PII in contravention of a company's privacy policy is itself an unfair and deceptive act. Presumably, the FTC would take the same position if the acquiring company ignored the policy once purchased (ignoring for the moment whether the FTC has such authority, a question being considered by the Third Circuit in the Wyndham litigation).

For example, in 2001 the FTC went to court to stop Toysmart from selling customer data in violation of its privacy policy. In that case, the FTC and Toysmart ultimately agreed that if the PII was going to be sold such a sale would need to meet the following conditions:

- The PII not be sold as a standalone asset;
- The buyer of the PII be engaged in substantially the same line of business;
- The buyer expressly agree to be bound by and adhere to the terms of the ToySmart's privacy policy; and
- The buyer agrees to obtain affirmative consent from consumers for any material changes to the policy that affect information collected under ToySmart's policy.

The FTC also sent letters objecting to proposed data sales in the bankruptcies of Borders, XY Magazine, and ConnectEDU. In Borders' bankruptcy proceeding in 2011, for example, the FTC took a position similar to that articulated in Toysmart. Borders issued a privacy policy in 2006, which provided that it would not disclose PII to third parties unless the customers expressly consented. A little over two years later, Borders issued another policy which added "Circumstances may arise where for strategic or other business reasons, Borders decides to sell...or otherwise reorganize its

business....In the event that Borders or all of its assets are acquired in such a transaction, customer information would be one of the transferred assets." Importantly, however, Borders also restated the consent requirements in this new, amended policy.

In a letter to the bankruptcy trustee, the FTC stated that it had brought "many cases" in which it alleged that the failure to adhere to a privacy policy constituted a deceptive practice under the Act and cited the Toysmart litigation. The letter demanded that the express consent be obtained and that the same conditions it successfully sought in Toysmart settlement be imposed. Thus, buyers and sellers can expect FTC scrutiny and involvement if there is any question that privacy policies are being violated.

And, of course there is the threat of customer litigation. Standing and damage requirements offer hurdles to such litigation. However, in Texas and Tennessee (and perhaps other states) the mere violation of the statute (and the policy) provides the requisite standing. Moreover, customers can claim that they paid for a product with the expectation that their privacy in connection with the transaction would be protected. Arguably, the violation of this expectation means they overpaid for the product and this provides the standing. As implausible as this sounds, similar theories have been asserted. See our recent post on automobile hackability:

<http://www.classcounselblog.com/hack-CAN-GM-Toyota-Ford>.

A sale of assets in contravention of the seller's privacy policy may also come with a threat of litigation.

The issues get even thornier in a third situation where the holder of the PII is in bankruptcy. How for example does a bankruptcy trustee meet its obligations to creditors while balancing the customers' privacy interests? Is there an obligation to sell the data in order to pay the creditors? What obligation does a bankruptcy trustee have to maintain customer privacy?

Certainly, bankruptcy courts have a great deal of leeway in overriding policies. Information, such as customer data, is an asset that is owned by the company. A bankruptcy court has an obligation to maximize the recovery of the creditors of a company — not an obligation to protect privacy interests of the bankrupt's

customers. And the Bankruptcy Act does leave the door open for the sale of such assets albeit with some safeguards.

The Act provides that if the debtor has a policy in place prohibiting the transfer of PII, the trustee may not sell such information unless that sale is consistent with the policy or after a hearing and the appointment of an ombudsman, the court approves the sale giving due consideration to the conditions for such sale and finding that the sale would not violate non bankruptcy law.

So at the end of the day, the final say so seems to be in the hands of the bankruptcy court itself, meaning the real losers could be the customers.

The potential pitfalls as demonstrated by these situations seem clear. So what's a business to do to minimize the risk?

- It should carefully prepare and review its privacy policies to see what obligations it might have upon a sell or transfer.
- If the business wants the freedom to sell the information it collects in the future, it should draft a policy accordingly.
- Notice of any changes to the policy giving it the right to sell its PII data should be prominently posted on its website.
- It should carefully consider what it is willing to do and not do with respect to its customers in the PII context.
- It should consider whether to clearly provide notice that bankruptcy or other economic or legal developments may occur and that such a scenario could affect what happens to the information.
- Businesses should take into account what possible liabilities and rights customers may have and what enforcement power the FTC has in evaluating the value and sale of PII.

And of course, the policy should take into account customers and their expectations: it does little good to create a "silver bullet" privacy policy that provides every protection to the business should it sell its assets if the end result is that it turns customers off!

If you have any questions regarding this Article or your rights in PII, please contact Steve Embry, with Frost Brown Todd LLC, at (502) 568-0253, or sembry@fbtlaw.com.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.