Commercial Data Privacy and Innovation in the Internet Economy:

A Dynamic Policy Framework

Issue Presented: Should baseline commercial data privacy legislation include a private right of action?

Position Statement: Joel Ruiz strongly urges the adoption of privacy legislation that includes a private right of action with statutory damages.

Interest of Commentator, Joel Ruiz

I am a citizen and resident of Texas and live in a town that nears the border with Mexico. Every day, I hear of illegal immigrants using falsified or purchased social security numbers to obtain work in my part of Texas. I have also read stories of individuals who have been wrongly accused of crimes after criminals stole their identities and committed crimes in their name. Jobs are hard to find in my area and the competition is keen.

In 2006, when I was unemployed and recently out of school, I applied to Gap, Inc. through their online application process for a position at its Old Navy brand. The website promised to protect my confidential information. It was the only means by which I could apply. However, in 2007, due to lax security by Gap's agent, laptops containing my social security number ("SSN"), address, and other sensitive information, as well as such information for 750,000 applicants, were stolen. The agent had (a) held on to the data longer than what Gap promised, (b) had not secured the laptops as industry, state, and Federal Trade Commission ("FTC") guidelines suggest, and (c) had failed to encrypt the data as industry, state and FTC guidelines suggest. In fact, the agent was running an analysis on the data for marketing purposes—a use for which Gap never obtained my consent.

As an expert opined in subsequent litigation I brought against Gap, this conduct increased my risk of identity theft and fraud by a ratio of 4-to-1. Gap offered a one-year credit monitoring program. However, as even the FTC has acknowledged, SSNs never expire, and thieves can hold on to the stolen data for years. So while the credit monitoring was inadequate, I tried to sign up anyway. However, due to wrong passwords, bugs in the system, incorrect advice from customer service representatives, and a lack of sufficient credit history, I was never able to sign

up for this free monitoring. Thus, in addition to all the time I spent, the minutes I expended on my cell phone, charges for faxes and scanning to establish my claim, I had no choice but to pay out-of-pocket for my monitoring despite my financial status.

The Need for a Private Right of Action

While the court found that I had standing to stay in court, it nevertheless held that I was not "injured" by Gap or its agent. *Ruiz v. Gap, Inc*., 380 Fed. Appx. 689 (9th Cir. May 28, 2010). I have to now, for the foreseeable future, monitor my credit closely, order credit reports, continue to purchase a credit monitoring package, and wait in fear of having my identity stolen by lawful or unlawful immigrants or by criminals who will use my name in their misdeeds. How this cannot constitute an "injury", I do not understand. In short, Gap and its agent ignored all the guidelines, took no precautions with information they mandated I give them, held on to it longer than they should have, used it in ways of which I never approved, and when the lax security permitted a thief to simply walk into an office and walk off with the information, I, and not Gap, were left holding all the financial responsibility.

In addition, public policy favors allocating the risk of loss to corporations like Gap, who are best able to prevent the loss or spread the loss. The corporations are clearly the only parties who could have prevented the loss by taking the necessary measures to maintain the security of the sensitive information with which it was entrusted. There is nothing the employee (or applicant as in my case) could have done to prevent this loss. In addition, if such a loss could not have been prevented, then surely large corporations, who benefit immensely in the financial sense from its employees' services, should be required to internalize the costs of this security breach, instead of spreading and externalizing the cost to their hapless employees.

The law, as it has been applied to date, has permitted companies to externalize on its employees all the costs and burdens of its own negligence and breach of contract by failing to keep confidential information safe as promised. While courts have tried to fashion a remedy with the current law available, data breach victims are still left without recourse. It is time for a legally created redress that an individual can use to protect their personal information and recoup their losses from those at fault for the data breach. The proposed statute either has to expressly recognize increased risk as an injury with credit monitoring and related insurance as damages, or

it has to provide statutory damages to anchor the claim and permit an employee to add his or her out-of-pocket losses.