TRAVEL LAW: ARE TOURISTS SAFE FROM HACKERS AND NEGLIGENT SUPPLIERS

August 25, 2014

By Thomas A. Dickerson

Nearly a billion people worldwide travel every year and in doing so entrust to airlines, cruiselines, hotels, rental car companies, tour operators and travel agents personal information regarding their identities including social security numbers, credit card numbers and so forth, all of which is of value to governments, hackers, marketers and competitors. How safe is your personal information from being taken without your knowledge or consent?

Airlines & The Government

In 2005 there were several class actions brought by passengers claiming that some airlines invaded their privacy and made available to the U.S. government their personal information [see *In re JetBlue Airways Corp. Privacy Litigation* ("Plaintiffs claim that defendant [violated their] privacy rights by unlawfully transferring their personal information to [Torch

Concepts, Inc.] for use in a federally-financed study on military base security. Plaintiffs seek a minimum of $1,000 in damages per class member"; complaint dismissed); *In re American Airlines, Inc. Privacy Litigation* (class action by passengers "allegedly injured when defendants...authorized Airline Automations, Inc. to disclose highly confidential passenger information-passenger name records...to (TSA) without the passenger's consent"); *In re Northwest Airlines Privacy Litigation* (class of passengers alleged "invasion of privacy, trespass to property, negligent misrepresentation, breach of contract and breach of express warranties [because] Northwest's website contained a privacy policy that stated that Northwest would not share customers' information except as necessary to make customer's travel arrangements" and violated policy by making information available to NASA which was studying ways to increase airline security; complaint dismissed); *Dyer v. Northwest Airlines Corp.* (class of passengers allege violation of Electronic Communications Privacy Act for disclosing private information without consent; complaint dismissed)].

Rental Car Companies

In *Najarian v. Avis Rent A Car System* "defendants printed the expiration date of Plaintiff's VISA card on a Check Out

Rental Agreement provided to Plaintiffs...(who) allege that defendants knew or recklessly disregarded that its use of cash registers that did not comply with the law and that [by] printing of Prohibited Information on customer receipts and thus defendant's (alleged) violations of the Fair Credit Reporting Act (FCRA) were 'willful' for the purposes of the FCRA"; class certification denied).

Hotels: Hackers Are Welcome

Recently some hotels have been the subject of "data breaches" by hungry hackers. In *Federal Trade Commission v. Wyndham Worldwide Corporation*, the FTC charged that a hospitality company and its subsidiaries engaged in unfair and deceptive trade practices in violation of the Federal Trade Commission Act by failing to maintain reasonable data security to protect guests from theft of their personal information.

Wyndham's Computer System & Websites

"Wyndham Worldwide is in the hospitality business...Under these agreements (defendants) require each Wyndham-branded hotel to purchase-and 'configure to their specifications'-a designated computer system that...handles reservations and payment card

transactions. This system ('property management system') stores consumers' personal information, 'including names, addresses, email addresses, telephone numbers, payment card account numbers, expiration dates and security codes'...computer network 'includes its central reservation system' that 'coordinates reservations across the Wyndham brand' and, using (defendants') website, consumers can make reservations at any Wyndham-branded hotel'"

Failure To Provide Reasonable Security

"The FTC alleges that, since at least April 2008, Wyndham 'failed to provide reasonable and appropriate security for the personal information collected and maintained by (defendants)...' by engaging in a number of practices that, taken together, unreasonably and unnecessarily exposed consumer personal data to unauthorized access and theft'. As a result...Between April 2008 and January 2010 intruders gained unauthorized access-on three separate occasions to (defendants') computer network".

Data Breaches & Damages

"The three data breaches (caused) the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain

registered in Russia, fraudulent charges on many consumers' accounts and more than $10.6 million in fraud loss. Consumers and businesses suffered financial injury, including, but not limited to, unreimbursed fraudulent charges, increased costs and lost access to funds or credit".

Unfairness: Data Insufficiencies

The Court found that the FTC sufficiently pled claims under the FTC Act for unfairness by specifically setting forth data security insufficiencies which included (1)"failing to employ firewalls; (2) permitting 'storage of payment card information in clear readable text'; (3) failing to make sure Wyndham-branded hotels 'implemented adequate information security policies and procedures prior to connecting their local computer networks to (defendants') computer network'; (4) permitting Wyndham-branded hotels 'to connect insecure servers to (defendants') networks, including servers using outdated operating systems that could not receive security updates or patches to address known security vulnerabilities'; (5) permitting 'servers on (defendants') networks with commonly-known default user Ids and passwords'; (6) failing to 'employ commonly-used methods to require user Ids and passwords that are difficult for hackers to guess'; (7) failing to 'adequately inventory computers connected to (defendants')

network' to manage devices on its network; (8) failing to 'monitor (defendants') computer network for malware used in a previous intrusion and (9) failing to restrict third-party access 'such as by restricting connections to specified IP addresses or granting temporary, limited access, as necessary".

Deception: Misrepresentations

The Court also found that the FTC sufficiently pled deception. "In this claim, the FTC cites the Defendant's privacy policy disseminated on (defendants') website and alleges that 'in conjunction with the advertising, marketing, promotion, offering for sale, or sale of hotel services. Defendants have represented, directly or indirectly, expressly or by implication, that they had implemented reasonable and appropriate measures to protect personal property against unauthorized access'-but that 'Defendants did not implement reasonable and appropriate measures to protect personal information against unauthorized access'. Accordingly, the FTC alleges that Defendants' representations 'are false or misleading and constitute deceptive acts or practices'". See also: Soloway & Bernstein, *Protection of Hotel Guest Data and Personal Information*, New York Law Journal (8/20/2014).

Other Privacy Cases

There have been other privacy cases involving unauthorized recordings by hotels [see e.g., *Simpson v. Vantage Hospitality Group, Inc.* ("This class action arises out of Defendant's alleged policy and practice of recording and/or intercepting calls made to a hotel reservation hotline without the consent of all parties..Plaintiff alleges one claim for unlawful recording and intercepting of communications pursuant to Cal. Pen. Code...and seek an award of statutory damages ($5,000 per violation)"; motion to dismiss denied); see similar cases: *McCabe v. Six Continents Hotels, Inc.* and *Roberts v. Wyndham International, Inc.*], sale of confidential medical information by pharmacies [see e.g., *Anonymous v. CVS Corporation* (sale of confidential information by pharmacy going out of business to pharmacy chain without consent of customers; causes of action for breach of fiduciary duty, breach of implied contract and violation of New York consumer protection statute stated; class certification granted)] and more hacking [see e.g., *In re Sony Gaming Networks and Customer Data Security Breach Litigation* ("This action arises out of a criminal intrusion into a computer network system used to provide online gaming and Internet connectivity via an individual's gaming console or personal computer")] and a more traditional and non-Internet invasion of privacy in a hotel [see

e.g., *Carter v. Innisfree Hotel, Inc.* ("Guest sued hotel for invasion of privacy, breach of contract, negligence, fraud and outrage in connection with alleged 'peeping Tom' incident in hotel)].

Conclusion

Given the aggressive and seemingly unstoppable efforts of hackers to access personal information, tourists are well advised to be very careful, indeed, in making such information readily available.

Justice Dickerson been writing about *Travel Law* for 39 years including his annually updated law books, *Travel Law*, Law Journal Press (2015) and *Litigating International Torts in U.S. Courts*, Thomson Reuters WestLaw (2015), and over 350 legal articles.