Delta Innovations & Privacy Law

Sean Davis

Full Sail University

Advanced Entertainment Law

28 March 2020

Delta Innovations & Privacy Law

When entering an industry, whether it be as an entrepreneur or through expansion, it is vital to assess one’s legal liabilities. A tried and true method is to analyze existing and prior court cases involving the target industry to look at litigation cases and decisions. This paper will break down a single case involving the IT industry concerning privacy data, by going through the facts of the case, issues of law, analysis of the case, and how it can apply to the Delta Innovations (DI) business model.

The case in question is that of Yershov v. Gannett in the US District Court of Massachusetts in 2015, and the subsequent appeal with the US Court of Appeals for the First Circuit in 2016 (Saylor, 2015; Thompson, O., Souter, D., & Kayatta, W., 2016). The case was initiated by the plaintiff named Alexander Yershov, which was a putative class-action lawsuit against the defendant Gannett Satellite Information Network, Inc. The plaintiff had downloaded the defendant’s mobile application *USA Today*,which contained news offering like that of the newspaper and broadcast media of the same name. The mobile application offers articles, pictures, audio, and video on a variety of topics all free of charge. The plaintiff alleged that the mobile application transmitted the mobile device identification (ID) and global positioning system (GPS) coordinates of user’s phones to a third-party company which, among other services, provides third party data analytics (Saylor, 2015).

In the complaint, Yershov asserts that the third party Adobe collects vast amounts of user data that can, combined with the device ID and GPS data, be directly linked to the identity and behavior of an individual, constituting it as personally identifiable information (PII) (Saylor, 2015). Additionally, the plaintiff argued that the videos itself are protected as private information per the Video Privacy Protection Act (VPPA) of 1988 (18 U.S.C.S. § 2710, 2013). The plaintiff includes all persons in the US who have used the app as part of the class in the suit (Saylor, 2015).

The statue in question originated in 1988 following the release of a Supreme Court nominee’s video rental history by a newspaper. In it the protections prohibit companies with interstate and/or foreign commerce involving renting, selling, or delivering video or audio-visual media from disclosing a consumer’s PII and/or viewing history without express written consent (Saylor, 2015; 18 U.S.C.S. § 2710, 2013). The same act states that a PII violation includes information which identifies an individual who has requested or acquired services from that medium unless it falls under five specific circumstances. Those circumstances are the release of information to the consumer, someone the consumer granted consent, a law enforcement agency or a court with a warrant, or subpoena, if it is integral in the delivery of the service, or if it solely consists of the name and address of the consumer and the consumer has been notified (18 U.S.C.S. § 2710, 2013).

The criteria in the statute are important in this matter, as it was the grounds for the first case in Massachusetts to be dismissed, upon request of the defendant. The defense argued firstly that the information transmitted is not PII, therefore not protected in the act. The defendant did not refute that the video name and content, GPS coordinates, and the phone ID were transmitted to Adobe. However, the defense stated that an android ID cannot be considered PII as it cannot, on its own merits, identify a person and requires other, non-public, information. The plaintiff rebutted with the idea that a GPS coordinate can, with enough time, determine a person’s home address, which can be used to identify a person using public records. After examining prior case law, the court did find that this information could be considered personally identifiable (Saylor, 2015).

With the criteria for PII being vague enough to justify a trial the motion to dismiss hinged upon the second claim of defense that the user was not, by definition, a consumer or subscriber. VPPA defines a consumer as “Renter, purchaser, or subscriber of goods or services from a video tape service provider” (18 U.S.C.S. § 2710, 2013). Due to the act being drafted long before the digital age, and the new terminology that goes with it, the court used prior case law to determine that a subscriber or consumer requires one or more of the following criteria “payment, registration, commitment, delivery, and/or access to restricted content” (Saylor, 2015). The *USA Today* mobile application at the time did not require payment, registration, or any commitment whatsoever. That fact combined with the existence of mobile apps with the above criteria resulted in Judge Saylor granting the motion to dismiss.

After going through the appeals process the US Court of Appeals for the First Circuit overturned the dismissal one year later and remanded the trial to continue (Thompson, et al., 2016). Firstly, the court upheld the initial finding that a unique ID and GPS fits the definition of PII outlined in the VPPA, noting how easily GPS could be used with public records to identify an individual. Secondly, the appellate court found that through common definitions and dictionaries that a subscriber can consist of someone who receives a product through a specific medium. The court then backed up the ruling with legal precedent that granted a party the title of “subscriber” without monetary payment. The criteria of needing to register was covered by the fact that for the app the function the user had to disclose the device ID and GPS information even if it was done automatically (Thompson, et al., 2016).

This result paves the way for a lot of future case law and gives DI a clear example of the scope of law involved in the mobile industry. The first thing to be learned is that the scope can expand beyond what is ordinarily covered. A mobile app has a dedicated End User License Agreement (EULA), along with the terms of service for the mobile distribution platform such as Android or Apple Store. Once those contracts and stipulations are covered there is state law, federal law, and international law.

In DI’s base of operations in Orlando Florida, there is the Florida Information Protection Act of 2014 (FIPA) and the Florida Deceptive and Unfair Trade Practices Act (FDUTPA), which comes into effect for not following FIPA (Donaldson, 2019). The United States has the US Privacy Act of 1974 and the Children’s Online Privacy Protection Act (COPPA) (Green, 2019). The above case demonstrated that depending on the content provided by the mobile application, new codes and statues may apply. In the future, due to the progression of law, or even today, international sales constitute far more strict regulations on PII. An example of such is the European Union General Data Protection Regulation (EUGDPR), which greatly expands both the definition of PII, its restrictions, and the consequences of a breach (gdpreu.org, 2020).

More specifically the above case demonstrates the need for a proper EULA and required registration even if the intent is to be a free product. DI should disclose to all users exactly what information will be shared, and to whom. Any changes to the policies and procedures must first meet all the requirements outlined in contracts and regulations, followed by the informed acknowledgment of the changes of policy by the user. Additionally, DI should acquire and maintain a current and comprehensive cyber insurance, that covers everything from a privacy breach to social engineering, errors and omissions, network business interruption, and more (Burke, 2020).

This paper went through a case of privacy law concerning Delta Innovation’s future business model. This paper covered the facts of the case, issues of law, an analysis of the case and DI’s plan to avoid, mitigate, or litigate future risks concerning privacy law.

References

Burke, D. (2020). Cyber Insurance 101: What Cyber Insurance Covers, 2020. In *woodruffsawyer.com*. Retrieved March 28, 2020, from https://woodruffsawyer.com/cyber-liability/cyber-101-insurance-coverage-2020

Donaldson, H. (2019). What You Need to Know About Florida’s Information Protection Act of 2014 (FIPA). In *digitalguardian.com*. Retrieved March 28, 2020, from https://digitalguardian.com/blog/what-you-need-know-about-floridas-information-protection-act-2014-fipa

Green, A. (2019). Complete Guide to Privacy Laws in the US. In *varonis.com*. Retrieved March 26, 2020, from https://www.varonis.com/blog/us-privacy-laws/

Personal Data (2020). In *gdpreu.org*. Retrieved March 28, 2020, from https://www.gdpreu.org/the-regulation/key-concepts/personal-data/

Saylor, D. (2015) *Yershov v. Gannett Satellite Information Network, Inc.*, United States District Court for the District of Massachusetts. Retrieved Mar 28, 2020 from <https://advance-lexis-com.oclc.fullsail.edu/api/document?collection=cases&id=urn:contentItem:5G0J-5VY1-F04D-D0VC-00000-00&context=1516831>.

Thompson, O., Souter, D., & Kayatta, W. (2015) *Yershov v. Gannett Satellite Information Network, Inc.*, United States District Court for the District of Massachusetts. Retrieved Mar 28, 2020 from https://advance-lexis-com.oclc.fullsail.edu/api/document?collection=cases&id=urn:contentItem:5G0J-5VY1-F04D-D0VC-00000-00&context=1516831.

Video Privacy Protection Act of 1988 (2013), 18 U.S.C.S. § 2710. Retrieved Mar 28, 2020 from https://www.govinfo.gov/content/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap121-sec2710.pdf