Journal of Civil & Legal Sciences
ISSN: 2169-0170
Mini Review Open Access

The FTC's Expanding Role in Cyber Security: Monitoring Activities

Sheu Tien H*
Department of Law, Attorney, LL.M. in Corporation, New York, New York, United States

Abstract

The Federal Trade Commission (FTC) is the chief consumer cyber security regulator in the United States. Through its actions against unfair and deceptive practices, it regulates surveillance and creates cyber security law. This research paper aims to review the premise of the FTC's authority about its legitimacy on cyber security regulation. The paper then focuses on the FTC's regulation on monitoring business. Recently, its regulation has expanded from deceptive to unfair practices, particularly on spyware technology.

Keywords: Power; Consumer; Ambiguity; Scope; Challenges; Lawsuit

Introduction

In essence, the FTC has established its mandate to ensure companies follow their own privacy settings and establish proper monitoring practices. In the end, the paper analyses the different approaches to surveillance regulation, such as class action litigations and statutory prohibitions, and provides possible solutions to enhance FTC's cyber security regulations on monitoring software in the future.

I. The Legitimacy of the FTC Enforcement on Cyber security

The FTC has faced two major challenges on cyber security enforcement within two decades: the statutory authority and the proper standard to enforcement. Due to the increasing cases in the cyber security domain, the FTC has established its position as the de facto national consumer-facing cyber security regulator. Those challenges hence followed through the growing power of the FTC and formed the foundation for an effective cyber security regime.

1. Challenge 1: the FTC's Authority as a Cyber security Regulator

The FTC has long required companies to implement a comprehensive information security program. Its legal base for enforcement is on the Federal Trade Commission Act of 1914 which prohibits "unfair or deceptive acts or practices in or affecting commerce" (codified as amended at 15 U.S.C. § 45(a)) [1]. Without mentioning that the FTC is a consumer cyber security regulator, it has left the Commission vulnerable to challenge based on its scope of authority. In the lawsuit of the FTC suing Wyndham, a hospitality company and three subsidiaries, the FTC alleged that Wyndham's data security failures led to three data breaches at its hotels in less than two years. In the defending argument, Wyndham has challenged the FTC's authority on cyber security regulations, yet the court held that the FTC has statutory authority to regulate cyber security under unfairness. The court noted that ambiguity and flexibility were purposefully built into the FTCA and dismissed Wyndham's argument that the alleged conduct fell outside of the plain meaning of "unfair". Generally, the Wyndham case is regarded as an FTC victory on its statutory authority. It ensured that cyber security is subject to unfair practice under section 5 of the FTCA despite the ambiguity of unfairness. Afterward, the FTC even created a new generation of case law that reaffirms its broad powers [2]. Notably, however, the Wyndham court held that the source of the FTC's common law, such as agency guidebooks complaints and consent decrees, did not provide ascertainable certainty for Cyber security requirements. Such concern leads to the second challenge regarding the uncertain standard.

2. Challenge 2: the Break-Down on FTC's Reasonableness Standard

The FTC faced another challenge about that to what extent the FTC security program requirements are specific. The "uncertain" issue was addressed in the LabMD case in 2019, where the Eleventh Circuit held that the FTC's consent order against LabMD was void because the security requirements were not specific enough to be enforceable. After the FTC's reasonable approach failed to provide sufficient specificity on what constitutes unreasonable data security, its orders have been improved by requiring more specific safeguards as part of the cyber security program.

Discussion

Such programs include biennial third-party assessment, obligating the settling party to present the written data security program to its board and to have its senior officers annually certify compliance to the FTC in the following enforcement proceeding. However, some pointed out the recent shift from the reasonableness standard to individual enforcement demonstrates the limitation of this legal framework that the obscure standard is unlikely to result in effective or coherent cyber security. The dismissing reasonableness standard explains why the FTC makes different mandates case-by-case, which creates a "common law" regime with its interpretations on unfair practices. From the abstract standard to specific requirements, the FTC begins to exercise its regulatory power against relatively controversial commercial activities. Of course, monitoring business is one of the most common targets subjected to unfairness reviews and serves as a significant component in the FTC's evolution [3]. Hence, the next chapter focuses on the latest FTC cyber security standards and requirements on surveillance products. After discussing the cases, this section turns to how the FTC elaborates the scope of acceptable surveillance through policy.

II. The Insight of FTC's Role on Monitoring Business

The FTC's recent actions shield consumers from some invasive

***Corresponding author:** Sheu Tien Hsin, Department of Law, Attorney, LL.M. in Corporation, New York, New York, United States, Tel: +07186643522, E-mail: ts4574@nyu.edu

Received: 24-Sep-2022, Manuscript No. JCLS-22-76036; **Editor assigned:** 27-Sep-2022, PreQC No.JCLS-22-76036 (PQ); **Reviewed:** 10-Oct-2022, QC No. JCLS-22-76036; **Revised:** 15-Oct-2022, Manuscript No JCLS-22-76036(R); **Published:** 22 Oct -2022, DOI: 10.4172/2169-0170.1000353

Citation: Sheu Tien H (2022) The FTC's Expanding Role in Cyber Security: Monitoring Activities. J Civil Legal Sci 11: 353.

monitoring. Its mandate derives from the authority to prevent deceptive or unfair practices in commerce. Deceptive practices involve a representation, guarantee or omission that is likely to mislead a reasonable consumer. In regulating surveillance, a company makes policies that turn out to be misleading or deceptive practices. Unfair practice plays a more important role to those practices that cause substantial injury even without misleading policies. Such substantial injury must not be reasonably avoidable by consumers and that is not outweighed by countervailing benefits to consumers or competition [4]. As the FTC polices insecure products or services, it interprets the FTC Act to require companies to employ reasonable cyber security precautions. The unfairness authority becomes powerful because it can address practices even if there is no relationship directly between the company and the consumer, such as those actions from the developers that facilitated the monitoring software. From a consumer perspective, the FTC's regulation on surveillance falls into the direct liability (such as tracking online and physical activities or using spyware) and indirect liability (such as installing insecure services or facilitating improper data transfers), with a distinction on whether its practices actively involve monitoring activities with consumers. The FTC has brought a series of cases against monitoring activities and has created a common law regime for this industry.

1. Tracking Online Activities

The deceptive misrepresentation about tracking is the most basic and easy case for the FTC to raise against other companies. Since it is easier for the FTC to decide whether the companies follow their own privacy policy, the FTC tends to cite its concept of "deceptive practices" to regulate the monitoring business. For instance, in a cross-device tracking case, Turn Inc. kept tracking the consumers even after they opted out of such tracking. The company privacy policy stated that consumers could block tailored advertising by using their web browser setting to limit cookies. However, the opt-out mechanism only applied to mobile browsers and Turn Inc. still used unique identifiers to track customers even after they blocked cookies from websites. The FTC alleged this was a deceptive practice because it misrepresented the scope of opt-out. "History sniffing" is also regulated under FTC norms. In Epic Marketplace, a company used the technique that allows online operators to determine what sites consumers have visited in the past. Epic not only collects consumers' information within the Epic Marketplace network as its policy stated. In fact, Epic used a history sniffing technique to collect information on websites outside of its network [5]. The FTC believed its practice was deceptive since it collected information beyond the scope authorized by consumer consent. Besides affirmative misrepresentation, ambiguous and incomplete disclosures are also defined as deceptions. The FTC has expanded the deceptive standard to practices that might have violated consumer expectations. Such omissions in disclosure may be deceptive. The most controversial example can be seen in the FTC's complaint against the Sears Holdings Management Corporation, owned by the department store company Sears. Sears offered a promotion to some online customers, which gave them the opportunity to be paid ten dollars in exchange for installing software that monitors user's online activities. Although data selling transactions is not prohibited, the FTC however found it deceptive because the extent of tracking was not sufficiently disclosed. While Sears revealed the money in exchange for "confidential tracking" of online browsing, the scope of data collected only appeared in the licensing agreement. Consumers might find the data surveillance far beyond their reasonable expectation. Similarly, in Chitika, a company offered consumers the choice to opt-out of its online network advertising. However, it did not disclose to consumers that the opt-out cookie would expire and disappear from their browsers only 10 days after being set. The FTC therefore believes Chitika's actions constituted deceptive practices. These cases suggested that the FTC cannot promise privacy protection and then actively undermines its effort through another undisclosed technique.

2. Tracking Physical Activities

Thanks to wireless networks and portable devices, the surveillance business turns its focus on consumers' offline activity information. Such information includes geo-location, physical transactions, or real-life activities. A tracking company can create a database built on information collected from consumers who allow the company access to their geo-location information, combining that data with the wireless networks they are near to document the physical location of wireless networks themselves. This company then would use that database to infer the physical location of consumers based on the networks they were near, even when consumers had turned off location collection on their device. Many advertising companies then analyse such data and serve ads to consumers based on their current locations. Without any warning, consumers would be surprised that the monitoring software follows them in the real world [6]. To meet a reasonable consumer's expectation, the FTC has imposed a stricter standard on advertising companies who own geo-location data. The FTC requires the monitoring companies to conduct surveillance within the data subject's expectation. For example, In Mobi, a mobile advertising company, had a privacy setting that would only track consumers' locations when they opted in and in a manner consistent with their device's privacy settings. However, In Mobi tracked consumers' locations, via the Wi-Fi network to which a consumer's device was connected or in-range, even if the consumer had not provided opt-in consent to access their location information. The FTC found these acts as deceptive practices because it fell beyond the app users' expectation.

This case provides two important messages for the mobile surveillance business:

[1] First, even a business-to-business mobile advertising provider (like In Mobi, who never dealt with mobile device users, only app developers) has the obligation to provide a privacy setting within the app users' expectation.

[2] Second, the FTC closed the door for even an indirect approach to acquire consumer's geo-location data through WiFi address, even the ability to infer locations from Wi-Fi data has not been a secret. Critics then questioned how InMobi could have deceived app users with whom itnever dealt, and readily available IP addresses can also narrow down users' location even without WiFi data [7].

Another example of online advertising platform is OpenX Technologies Inc. (OpenX).OpenX's Ad Exchange platform connects websites and apps publishers with advertisers who wish to display targeted advertisements. In violation of its privacy setting, OpenX collected precise location data, i.e., BSSIDs, from consumers who have opted out of such collection. It was also discovered that, notwithstanding OpenX's inclusion of location permissions in theOpenX Android SDK code, OpenX used a backdoor method to retrieve the BSSID. Google then notified OpenX that its Android SDK was acquiring location data using the BSSID in a non- sanctioned manner that violated Google's Device and Network Abuse Policy. The FTC alleged that it was deceptive when OpenX misrepresented its data collection practices and collected consumer location data when the consumer had not provided consent or had expressly deniedconsent.

In this case, the FTC also emphasizes that

[1] Even a business-to-business advertising provider (like OpenX, who never dealt with mobile device users, only app publishers and advertisers) has the obligations to provide a privacy setting within the app users' expectation and

[2] Advertising provider should explicitly express the approaches to geo-location data collection, without using any undisclosed collecting means. In addition, tracking consumers' physical movement is also within the FTC's regulatory domain [8]. Nomi Technologies is a company whose technology allows retailers to track consumers' movements through their stores. Its privacy policy promised that Nomi would provide an opt-out mechanism at stores using its services and implied that consumers would be informed when stores were using Nomi's tracking technology. However, no in-store opt-out mechanism was available, and consumers were not informed when the tracking was taking place. The FTC claimed the representation was false and misleading which constituted a deceptive act.

3. Computer Spyware

The FTC has put the brakes on the business practices of an operation that was selling spyware and showing customers how to remotely install it on other people's computers without their knowledge or consent. The standard of fair practice was established through spyware cases. In Cyber Spy Software, a company sold Remote Spy, a key-logger software program on computers that was touted as a 100% undetectable way to spy on anyone from anywhere. Cyber Spy Software provided their clients with detailed instructions explaining how to disguise the spyware as an innocuous file, such as a photo, attached to an email. When the email recipient clicked on the attachment, the Remote Spy program was downloaded and installed without the victim's knowledge and cannot be readily located or uninstalled by the owner [9]. Cyber Spy even provided a configuration wizard, a user tutorial, and step-by-step instructions demonstrating how to deploy the software without the computer owner's knowledge or authorization. The spyware recorded every keystroke typed on an infected computer; captured images of the computer screen; obtained passwords, and recorded websites visited.

The FTC alleged that those practices were unfair in three aspects:

[1] Unfair sale of spyware that can be installed without the knowledge and consent from the owner of an infected computer to monitor its activities.

[2] Unfair collection and disclosure of consumers' personal information without the authorization from the computer users

[3] Unfair means to install spyware and access consumer's personal information [10]. After the FTC filed a complaint for permanent injunction and other equitable relief against Cyber Spy, the court ordered Cyber Spy to take further steps to protect the computer users and implement a license system prohibiting a single licensed copy of the software from being used on more than one computer at any given time.

Based on the order, Cyber Spy must

[1] Provide installation notice with a clear choice either to install or not install the software and the install button or option may not be highlighted,

[2] Provide a system tray icon appearing in the task bar on the user's desktop when the software is running,

[3] Provide the user with clear and prominent information sufficient to identify how the users can contact Cyber Spy for additional information or to resolve an issue of improper installation of the software,

[4] Provide a link to disable the installation of the software. The FTC prohibits the monitoring technology from tracking geophysical location without the consent of the users. In Designer Ware, a company marketed a program that enabled companies to track the physical location of rent-to-own leased computers. Designer Ware recommended, but did not require, that rental companies disclose the presence of software [11]. Such software, however, collected personal information from the rented computers and tracked the geophysical location of computers without either users' consent or notice. The FTC alleged such engagement in secret monitoring and data collection was unfair and demanded a clear and prominent notice, affirmative express consent, and the icons on the screen.

4. Stalking Apps

The FTC also brought cases against developers of stalking apps and curved out companies' impermissible cyber security practices such as

[1] Selling stalking apps that circumvent security protections on mobile devices or

[2] Failing to ensure the users with legitimate ground for monitoring. Unlike the monitoring software discussed above which were viewed as deceptive, the FTC focuses on "unfair practices" to build reasonable regulations on stalking software. Failure to follow secure practices can be compounded to vulnerable cyber security. In Retina-X, developers launched three mobile device apps that allowed purchasers to monitor the mobile devices on which they were installed, without the knowledge or permission of the device users. Purchasers can access sensitive information about device users, including the user's physical movements and online activities [12]. To install the apps, the purchasers were required to bypass mobile device manufacturer restrictions. The FTC alleged that circumventing security protections implemented by the mobile device operating system and did so without taking reasonable steps to ensure that the monitoring products will be used only for legitimate and lawful purposes by the purchaser exposed the devices to security vulnerabilities.

Retina-X was also accountable for making a dangerous product for other reasons.

[1] Its design failed to take any steps to ensure its apps were being used for only employees and children monitoring.

[2] In addition, each of the apps provides purchasers with instructions on how to remove the app's icon from appearing on the mobile device's screen. These apps run surreptitiously in the background and are uniquely suited to illegal use.

[3] The apps are exposed to security vulnerabilities. Between February 2017 and 2018, the hacker accessed data collected through these apps including login usernames, encrypted login passwords, text messages and GPS locations and photos [13]. This cyber security incident emphasized that Retina-X and Johns failed to adequately secure the information collected from the mobile devices.

[4] Moreover, Retina-X outsourced most of its product development and maintenance to third parties and failed to adopt and implement reasonable information security policies and procedures. The FTC therefore concluded Retina-X's actions are unfair practices, which cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition [14]. In 2020, Retina-X reached a settlement with the FTC over allegations that the company and its owner Johns failed to secure the data collected by its "stalking" apps and ensure the apps were used

for legitimate purposes. In the consent decree, Retina-X and Johns must require purchasers to state that they will only use the app to monitor a child or an employee, or another adult who has provided written consent. They must include an icon with the name of the app on the mobile device, which is only removable by a parent or legal guardian who has installed the app on their minor child's phone. The settlement also required Retina-X and Johns to delete the data they collected from the stalking apps and prohibits Retina-X and Johns from promoting, selling, or distributing any monitor app that requires users to circumvent a device's security protections to install it. In terms of cyber security requirements, Retina-X and Johns must implement and maintain a comprehensive information security program designed to protect the personal information they collect. Such a program must include specific safeguards to address the security issues identified in the agreement and obtain third-party assessments of their information program every two years. Similarly, Support King (SpyFone.com) also launched a stalking app that allowed purchasers to monitor user devices. Its app also requires purchasers who used the apps on Android devices to bypass the restriction on devices with instructions on how to hide the icon. The secret surveillance provided by the apps exposes the device user to potential stalking. The FTC therefore claimed Support King failed to protect the personal information collected by the app despite promising it took "reasonable precautions and safeguards." Other security deficiencies included not encrypting personal information stored; failing to ensure that only authorized users could access personal information and transmitting purchasers' passwords in plain text. The vulnerable cyber security led to the fact that the hacker accessed the company's server and stole personal data. After the cyber incident, the company promised purchasers it would work with an outside data security firm to investigate; however, it still failed to follow through. In 2021, the FTC filed the complaint alleging that selling stalking apps without taking reasonable steps to ensure the purchasers' use the monitoring products for legitimate purposes constitute unfair acts or practice. In addition to banning the company from selling any surveillance app, the proposed settlement requires them to delete any information illegally collected from the stalking apps. It also ordered to notify the owner of devices on which the apps were installed that their devices might have been monitored and the devices might not be secure. At the time this article is written, Support King has not reached an agreement with the FTC yet. Both Retina-X and Support King Cases embody that the FTC's regulation is shifting from preventing deceptive practices to enforcing fair practices. The fair commercial practices for stalking app developers mean not to circumvent any device's security protections, to ensure the user with legitimate reasons to monitor others and to include an icon with the name of the app on the mobile device as a default rule.

III. The Future Cyber security on Monitoring Business: Policy and Regulation

This chapter analyses the different approaches to surveillance regulation, such as class action litigation and statutory prohibitions, and provides possible solutions to enhance FTC's cyber security regulations on monitoring software in the future.

1. The Rethink of Cyber security Regulatory Regime

In an attempt to regulate cyber security, the FTC regulatory common law is not the only approach. Different approaches such as class action litigation and statutory prohibition also play their roles in the cyber security regulatory regime. It then raised the question that is there any other regulatory approach that fits better than the FTC's role as a main cyber security regulator. To answer the question, making a comparison between different systems helps analysis. First, the system of class action litigation filed after a cyber-security incident serves as a common law regulator. However, the cyber security litigation is extremely difficult to mount. The victims who have been monitored often do not realize the problem until the breaking news and rectifying it through a litigation often requires a new invasion of privacy, such as putting the materials of their privacy lives collected from stalking software into public legal complaints. The victims may also be dis-incentivized by a small amount of compensation compared to the cost of suit. The FTC could have filled the plaintiff litigation void through its investigation and negotiation power. The FTC investigations can find the vulnerable monitoring practices before either a cyber-attack or a data leak, which prevent the damages before actual hazard. On the other hand, companies choose to settle matters because the selected FTC's cases are generally obvious violations of FTCA and because the FTC investigations typically unearth more wrongdoing than it initially suspected. In other words, what the FTC's can do outweighs the one in class action suits. Second, the statutory prohibitions for cyber security may seem to be another alternative. In fact, the FTC has published its cyber security guideline, Protecting Personal Information: A Guide for Business, which describes a checklist of practices that form a sound data security plan [15]. The guidebook does not state that any particular practice is required, but it does counsel against many of the specific practices. For instance, it recommends that companies consider encrypting sensitive information that is stored on a computer network, check software vendors' websites regularly for alerts about new vulnerabilities and implement policies for installing vendor-approved patches. However, in Wyndham, the court held that the FTC's guidebook could not, on its own, provide "ascertainable certainty" of the FTC's interpretation of what specific cyber security practices. In addition, in February 2013, President Obama issued Executive Order 13636, "Improving Critical Infrastructure Cyber security," which called on the Department of Commerce's National Institute of Standards and Technology (NIST) to develop a voluntary risk-based Cyber security Framework for the nation's critical infrastructure. However, the FTC alleged that the Framework is not, and isn't intended to be, a standard or checklist. It's meant to be used by an organization to determine its current cyber security capabilities, set individual goals, and establish a plan for improving and maintaining a cyber-security program, but it doesn't include specific requirements or elements.

So why not elevate the guidelines into statutory rules? The potential reasons may be

[1] The difficulty for bipartisan approval of the cyber security statute,

[2] The conflicted power between the federal and state cyber security authorities and

[3] The need for flexibility in face of the changes in the cyber security.

The court has recognized that there is no such thing as perfect security, and that security is a continuing process of detecting risks and adjusting one's security program and defences. Therefore, as the FTC provides ascertainable certainty of the interpretation, the section 5 of the FTC Act remains as a primary enforcement tool that the FTC relies on to prevent deceptive and unfair practices.

2. The Policies for Future Cyber security Regulations on Monitoring Software

(1) Ensuring a Valid Consent from Monitoring Subjects

In the view from consumers, cyber security represents not only the vulnerability toward cyber-attacks but also the unauthorized

data theft from the monitoring companies. To reduce the unwitting data collection, the quality of the consumer consent is the key. A full consideration of consent would include whether there is adequate information about data collection, whether consent is voluntary, whether the user has the competence to consent (e.g., the minors) and the terms of withdrawal of consent. The FTC has pushed the monitoring business to provide a clear and prominent notice, an affirmative express consent, and the icons on the screen in exchange for a valid consent. Sometimes consent from the user is not enough when the service causes cyber-vulnerability. The FTC has prohibited the software that bypasses a safety protective system even if a user who receives instructions agrees on it. In the future, the FTC will keep elaborating what a fair practice should be and how a valid user consent works when monitoring activities involved.

(2) Leveraging CISA Programming to Improve the FTC Cyber security Enforcement

The collaboration between the governmental departments will be a solution for future regulation. Through the collaboration with other authorities with specific standards, the FTC may adopt specific cyber security standards which benefit its enforceability. The Cyber security and Infrastructure Security Agency (CISA) under the Department of Homeland Security (DHS) is a good choice for collaboration. As an agency to improve domestic government and private-sector cyber security, CISA offers a range of services designed to prevent and mitigate cyber-attacks. However, the engagement with the agency is voluntary and it faces a problem: few economic incentives are provided for a private company to share its cyber security related information. While the FTC needs specific cyber security regulations to provide notice and enforceability, CISA needs a way to encourage greater private-sector engagement with its programs. Hence, linking FTC enforcement with CISA standard would be a win-win situation. An FTC order embracing CISA programming with CISA tools creates a clearer and more administrable order [16]. Since CISA provides specific anticipation based on the industries, it will lead to a more foreseeable standard for monitoring business.

(3) Reminding Potential National Security Concerns with Monitoring Technology

Although the FTC focused its regulations on consumer protections so far, it is possible that the monitoring technology raises national security concerns. The use of tracking or remote access to systems supporting the operation of critical infrastructure or national critical functions will be dangerous if under cyber-attack or bad monitoring practices. To reduce the damages, it requires the FTC to collaborate and coordinate with other cyber security enforcement authorities (e.g., the FBI, DHS or DOD) who have situational awareness, effective risk management programs, and protective measures. Information shared within cyber security enforcement authorities through structured and secure information sharing environment helps to build a safer net for cyber security against monitoring interference.

IV. Conclusion

The FTC has established its cyber security regulations through unfair and deceptive practice reviews of tracking activities. Despite most of the cases being settled with the FTC, the cases brought to courts challenging the FTC regulatory authority and unenforceable requirements, have made the FTC tailor its cyber security enforcement to be more specific. At the same time, the FTC expanded its fairness reviews meeting higher consumer expectations nowadays. Such rulings include a ban on the spyware circumventing security protections on the device and a requirement for monitoring companies to protect the consumer's privacy even under business-to- business transactions. That said, the advertising companies and the software developers together are responsible for privacy and cyber security protections for consumers. Besides the FTC's common law regime, the class action litigations and statutory prohibitions are possible approaches that provide protections for consumers. In a broader view, the call for cyber security requires the FTC to collaborate with other governmental authorities minimizing cyber security risks. Leveraging CISA programming will be one way for the FTC to build more specific and predictable requirements for monitoring activities. The potential national security risk through monitoring activities is another reason for a more sophisticated cyber security enforcement. Without doubts, the FTC's cyber security regulations will evolve in response to the new monitoring technology and means in the future

Acknowledgement

None

Conflict of Interest

None

References

1. Gamariel M, Claude KJ (2021) Influence of Public Procurement Regulations on Economic Growth of a Country, a Case of Rwanda Public Procurement Authority, Evidence 2015-2019. SSLEJ EU 6:726-738.
2. Scheltema M (2019) The mismatch between human rights policies and contract law: Improving contractual mechanisms to advance human rights compliance in supply chains. 1st Edn Routledge UK 1-20.
3. Haque AKE (2021) The Bangladesh Competition Law–Improving the Efficiency of the Market. Dh Univ L J IND 32: 1-12.
4. Sainati T, Locatelli G, Smith N (2019) Project financing in nuclear new build, why not? The legal and regulatory barriers. Energy Policy EU 129: 111-119.
5. Terrebonne RP (1981) A strictly evolutionary model of common law. J Leg. Stud US 10:397-407.
6. N Gennaioli, A Shleifer (2007)The evolution of common law. J Polit Econ US 115:1-27.
7. Goodman JC (1978) An economic theory of the evolution of common law. J Leg. Stud US 7:1 -393.
8. AJ Hirsch (2004). Evolutionary theories of common law efficiency: reasons for (cognitive) skepticism. Fla St U L Rev US 425: 1-40.
9. Ponzetto GAM, Fernandez PA (2008) Case law versus statute law: An evolutionary comparison. J Leg Stud US 37: 1-40.
10. Terrebonne RP (1981) A strictly evolutionary model of common law. J Leg. Stud US 10: 397-407.
11. Scarelli T (1959) Obbligazioni Pecuniarie (Geldschulden) (Artt. 1277–1284): Commentario del Codice Civile a cura di Antonio Scialoja e Guiseppe Branca. Nicola Zanichelli, Bologna, und Soc. Ed. del Foro Italiano. JSTOR NY 25: 343-346.
12. Ellona M (1971) Trattato della responsabilità civile. Milano UK 1- 20.
13. Cesareo F (2017) Astreintes and Italian Law, in Civil Procedure Review (2191-1339).Civ Pro rev UK 8:45-72.
14. Cupis A(1985) Sul tema del danno e del risarcimento. Milano UK:320-323
15. Betunio M (2017) Punitive damages. LUISS Eur Pri Law EU: 1-138.
16. Asatryan A (2019) Innovation in Public Procurement Process in Armenia: A Strategy for EU Integration. J public procur innov EU: 615-622.