INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 11 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

DIGITAL BAILMENT

AUTHOR - VIJAY PUJAR, STUDENT AT NATIONAL LAW SCHOOL OF INDIA UNIVERSITY BENGALURU

BEST CITATION – VIJAY PUJAR, DIGITAL BAILMENT, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (11) OF 2025, PG. 177-183, APIS – 3920 – 0001 & ISSN - 2583-2344

Abstract:

This research paper explores the concept of digital bailment, an evolving legal framework situated at the intersection of traditional bailment principles and modern digital realities. While bailment traditionally applies to tangible assets, this paper however investigates the legal viability of extending bailment doctrines to intangible assets such as electronic data. It critically analyzes key U.S. court decisions like Richardson v. DSW, Sony Gaming Networks and Target, where bailment claims over data breaches were rejected, and draws parallels with Indian jurisprudence, particularly the Supreme Court's ruling in Justice K.S. Puttaswamy v. Union of India regarding Aadhaar data retention. The paper further evaluates the duty of care expected from cloud storage providers and also critiques the proposition that such services fall within the scope of traditional bailment. It compares cloud storage with safe deposit boxes, highlighting distinctions in possession and control. The paper also engages with Shane Gallant's "Adhesion Bailment Doctrine" in the Internet of Things (IoT) context, proposing a theoretical safeguard against state surveillance. In conclusion, the paper advocates for legislative reform to incorporate digital bailments within the Indian legal system, thereby ensuring enhanced privacy and data protection in an increasingly digitized world.

Introduction:

A bailment is a delivery of property from one person to another for a specific purpose under a contract providing that the property will be returned when that purpose has been accomplished or the bailor reclaims the property.[337] In a time where there is rapid technological progress with great impact of digital resources, the idea of digital bailments arises as a by-product at the junction of law and technology. This concept of digital bailments works within the intersection of laws encounter the newer intricacies of the digital era. Digital Bailment has not been defined universally but one possible interpretation is temporary transfer of digital assets or information from one party to another on the same lines of traditional bailment principles but with respect to digital context.

Thematic approach/ Scope of the topic:

The scope of the topic is to try and explore the realm of digital bailment and try to establish that the traditional bailment can be extended to intangible assets like digital information and electronic data.

Question to be answered by this research paper are:

- The research paper in general would try to answer few of the questions and analyse the literature from the above sources and apply some to Indian context.
- Criticism of some of the judgements of US courts wherein intangible assets have not been granted traditional bailment will also be looked into and also how Indian courts can also find answers to such questions.
- Analyse if there exists connection between cloud storage and locker/safe

Adam J. Levitin, Not Your Keys, Not Your Coins: Unpriced Credit Risk in Cryptocurrency, 101 Tex. L. Rev. 923 (2023); United Truck Rental Equip. Leasing, Inc. v. Kleenco Corp., 929 P.2d 99, 103 (Haw. Ct. App. 1996)

deposit. Drawing of comparison between Indian and USA's position with respect to, duty of care.

Literature Review:

The literature talks about the modern definition of bailment expanding it to electronically stored data. Historically, bailment law only applied to tangible property such as chattels. Whether bailment applies to intangible property, such as electronic data, has long been a matter of substantial debate.[338] US courts have interpreted bailments of electronic data to include computerized data stored on a hard drive, information stored electronically on a computer, computer programs and financial data stored on a computer.[339] The literature further analyses if traditional bailment principles apply to electronically stored information. The questions regarding bailment theory to digital data after data security breach is also looked into.

The new bailment by Danielle D'Onfro questions some of the aspects of digital bailment and cloud storage and duty of care with in the realm of digital context. The author talks about whether the storage company can access the files under its care or whether those files are encrypted before the storage company has access to them. Here, the relevant encryption is not
the security measures that prevent unauthorized access to the files, but rather the security measures that prevent even the storage company from reading the data on its servers. For example, Apple famously uses end-to end encryption in its messaging app, making it nearly impossible for Apple to access users' data, even at the behest of law enforcement[340].

Shane Gallant in his journal proposes adhesion bailment doctrine. The "adhesion bailment doctrine" is premised on fairness and provides enhanced protection to the individual IoT user. Courts can use bailments as a way to clarify what privacy protection an IoT user maintains.[341] The author talks about the third parties or the intermediaries in the Internet of Things era acting as bailees. There are two ways one can view a service provider as a bailee. The first is viewing a third-party company as a intermediary, i.e., a bailee, who is provided the information to perform a task, rather than as the "recipient" of the information.[342] The author has analysed from the perspective of US Supreme court justice's theory on bailments and tried to extend its scope.

Identifying the gaps:

- The research paper in general would try to answer few of the questions and analyse the literature from these sources and apply some to Indian context.
- Criticism of some of the judgements of US courts wherein intangible assets have not been granted traditional bailment will also be looked into and also how Indian courts can also find answers to such questions.
- Analyse if there exists connection between cloud storage and locker/safe deposit.
- Briefly analyse Justice Neil Gorsuch's theory on bailments and its expansion by the author Shane Gallant calling it Adhesion Bailment Doctrine

The research paper will try and analyse different aspects of the gaps mentioned in the literature review paper and conduct a comparison where necessary and also criticise when there logically the USA's position seems appropriate. The basic theme would revolve around the duty of care

[338] William LaRosa, New Legal Problems, Old Legal Solutions: Bailment Theory as the Baseline Data Security Standard of Care Owed to an Opponent's Data in E-Discovery, 167 U. Pa. L. Rev. 792 (2019); Thyroff v. Nationwide Mut. Ins. Co., 864 N.E.2d 1272, 1275-77

[339] See David Barr Realtors, Inc. v. Sadei, No. 03-97-00138, 1998 WL 333954 (Tex. App. June 25, 1998)

[340] Danielle D'Onfro, The New Bailments (Wash. U. in St. Louis Sch. of Law, Working Paper, 2022) (on file with author); Caitlin Dewey, Apple's iMessage Encryption Foils Law Enforcement, Justice Department Complains, WASH. POST (Apr. 5, 2013), https://www.washingtonpost.com/business/technology/apples-imessage-encryption-foils-law-enforcement-justice-department-complains/2013/04/05/f4a6b66e-9d68-11e2-a2db-efc5298a95e1_story.html [https://perma.cc/4VRD-UCTD].

[341] Shane Gallant, The Old Bailment Doctrine: The Answer to Fourth Amendment Jurisprudence in the Digital Age, 25 Roger Williams U. L. Rev. 116, 144 (2020).

[342] See id ; This paragraph draws from Justice Gorsuch's theory on bailments and applies it practically in the IoT world.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 11 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

with respect to digital/electronically stored data between users and the companies that store these data and also how the courts can look into this area and find solutions in highly digitised world.

Research paper

Analysing the Digital Bailments Doctrine: Indian context vis-à-vis the USA

A bailment only applies to certain types of property. Historically, bailment law only applied to tangible property such as chattels.[343] Whether bailment applies to intangible property, such as electronic data, has long been a matter of substantial debate. For example, the Northern District of California previously concluded that social security numbers and credit card information are not bailable property. [344] Later courts have repeatedly held that electronic data may be intangible property subject to a bailment. Courts have interpreted bailments of electronic data to include computerized data stored on a hard drive, information stored electronically on a computer, computer programs, and financial data stored on a computer.[345]

The consensus of US courts in data security litigation has been that electronic data that is transferred does not constitute the "delivery" of property required for the creation of a bailment. The bailment theory to data breach was first addressed in Richardson v. DSW, Inc. In Richardson, a class of consumer plaintiffs sued DSW shoe shoppers under a bailment theory after a data security breach led to the dissemination of stolen credit and debit card information. The court rejected the plaintiffs' bailment theory.[346] The bailment theory to data security litigation first introduced in Richardson later resurfaced in Sony Gaming Networks and Target. Sony Gaming Networks involved a nationwide class action brought against Sony following a massive data breach. Hackers accessed Sony's network and stole the personal information of millions of Sony customers, including customers' "names, mailing addresses, email addresses, birth dates, credit and debit card information," and more.[347] The Sony court quickly dismissed the bailment claim, reasoning that the plaintiff's electronic personal information could not be "construed to be personal property so that the [plaintiffs somehow 'delivered' this property to Sony and then expected it to be returned."[348] Citing both Richardson and Sony Gaming Networks , the Target court rejected the plaintiff s bailment claims, reasoning that the electronic data that was stolen could not be returned to the bailor. However, the Target Court "provided essentially no analysis of **bailment claims, the standard of care applicable, or the issue of whether 'return of the property is an element at all, let alone where the property is intangible."[349]**

Companies like Target and Sony are not permitted to retain customer credit card and personal information indefinitely. The companies receive a digital copy of the information, but they certainly do not obtain an ownership interest over an individuals credit card or personal data. In some cases, these companies are required by law to destroy the credit card and personal data after a certain period.[350] Moreover, by destroying the data, they return to the customer the right (or fact) that they are the sole possessor of the personal data and information in question. [351]

[343]William LaRosa, New Legal Problems, Old Legal Solutions: Bailment Theory as the Baseline Data Security Standard of Care Owed to an Opponent's Data in E-Discovery, 167 U. Pa. L. Rev. 792 (2019).; Samuel Stoljar, The Early History of Bailment, 1 AM. J. LEGAL HIST. 5, 31-32 (1957)

[344] William LaRosa, New Legal Problems, Old Legal Solutions: Bailment Theory as the Baseline Data Security Standard of Care Owed to an Opponent's Data in E-Discovery, 167 U. Pa. L. Rev. 792 (2019); Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008)

[345] Ibid. 793; Bridge Tower Dental, P.A. v. Meridian Comput. Ctr., Inc., 272 P.3d 541, 546 (Idaho 2012)

[346] Ibid. 789; Hendricks v. DSW Shoe Warehouse Inc., 444 F. Supp. 2d 775 (W.D. Mich. 2006)

[347] Ibid. 789; In re Sony Gaming Networks and Customer Data Sec. Breach Litigation, 996 F. Supp. 2d 942 (S.D. Cal. 2014)

[348] Ibid. 789

[349] Ibid. 790; *In re Target Corp. Data Security Breach Litig.*, 66 F. Supp. 3d 1154 (D. Minn. 2014)

[350] Ibid. 790; INN. STAT. ANN. § 325E.64 (West 2007)

[351] Ibid. 790

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 11 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

For purposes of bailment liability, property is "damaged" when it is not returned in the same condition it was in when it was delivered. Data that has been hacked has been fundamentally and irreparably changed, and thus is not returned in the same condition that it was in when it was delivered. The author argues that, when electronic data is breached and accessed by hackers, it suffers a loss of value that equates to a damaged condition of the data.[352] Hence, it can be under the classification of bailment liability.

According to the Supreme Court of India, Aadhaar authentication data can only be retained for a period of **six months**. This means that any data collected during an Aadhaar authentication, such as the date, time, location, and biometric information of the person being authenticated, must be deleted after six months.

The Supreme Court made this ruling in 2018, in a case known as **Justice K.S. Puttaswamy v. Union of India**. The court found that retaining Aadhaar authentication data for longer than six months was a violation of the right to privacy. [353]

According to the author, if a bailment exists, four elements must be satisfied to bring a successful bailment claim for electronic data: "1) the existence of an agreement, express or implied, to create a bailment; 2) delivery of the electronic data; 3) acceptance of the electronic data by the bailee; and 4) nonreturn or redelivery of the electronic data in a damaged condition."[354]

Comparing the stances of both the United States and India on the aforementioned factors, it becomes evident that in the case of Justice K.S. Puttaswamy v. Union of India, the Supreme Court found that retaining Aadhaar authentication data for longer than six months violated the right to privacy. This finding underscores the significance of the deletion of authentication data, aligning with the notion that by erasing such data, companies effectively return to the customer the right or fact that they are the sole possessor of the personal data. This alignment resonates with the traditional understanding of returning goods in bailment cases. Despite the Supreme Court of India not explicitly expanding the concept of bailment in this context, one could interpret that, considering the Indian context, the act of deletion implies the restoration of exclusive possession and control to the rightful owner.

Thus, extending the concepts discussed above to private companies in India, specifically focusing on data deletion practices as a strategy to mitigate liability, coupled with enhanced contractual safeguards for customers, holds the potential to pave the way for a more robust framework in the realm of the Bailment of Digital Data. Comparing both the U.S. and Indian stances reveals common ground in recognizing the pivotal role of data deletion in restoring exclusive possession to the rightful owner. Extending these concepts to private companies in India, particularly emphasizing data deletion practices to mitigate liability, holds promise for shaping a more robust framework for the Bailment of Digital Data.

Addressing duty of care in cloud storage:

The new bailment by Danielle D'Onfro questions some of the aspects of digital bailment and cloud storage and duty of care within the realm of digital context. The author talks about whether the storage company can access the files under its care or whether those files are encrypted before the storage company has access to them. Here, the relevant encryption is not
the security measures that prevent unauthorized access to the files, but rather the security measures that prevent even the storage company from reading the data on its

[352] Ibid. 801; Brian T. Yeh, Protection of Trade Secrets: Overview of Current Law and Legislation, CONG. RES. SERY. 2 (2016)

[353] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, 283.

[354] Ibid. 800; Rachel M. Kane, Proof of Breach of Bailment in Cases Where Object of Bailment Is in Form of Electronic Data, 156 Am. Jur. Proof of Facts 3d 1, § 2 (2016) ("An action for breach of bailment may sound in either tort or contract, at the plaintiff's option.").

servers. For example, Apple famously uses end-to end encryption in its messaging app, making it nearly impossible for Apple to access users' data, even at the behest of law enforcement[355].

Where the cloud storage company receives payment whether in dollars or data from the users of its services, it is most analogous to a bailment for hire or bailment for mutual benefit. In these cases, the default rule would be that the bailee company owes its customers a duty not to act negligently with respect to the stored data. This standard might compel firms to maintain security protocol at least at industry norms and, more importantly, respond more promptly to reported security flaws.[356] With cloud storage, customer error often creates the breach or mis-delivery. A strict liability rule is more difficult to justify on these facts unless it is reserved for data breaches in which there is no customer error. [357]

My critique of the duty of care in the digital bailment of cloud storage data lies in the fact that some cloud storage company can disclaim liability for negligent acts by exculpatory clauses in their contractual agreements. But I would agree to the authors idea that giving consumers the option to buy insurance for an additional fee may increase the likelihood that a court will enforce the exculpatory clause.[358] My critique of the duty of care in the digital bailment of cloud storage data centres on the issue that some cloud storage companies can disclaim liability through exculpatory clauses in their contractual agreements

Analysing safe deposit boxes and cloud storage on possession and control:

Safe deposit boxes are secure lockers held in a vault, often at a bank but sometimes at a stand-alone safe deposit company. These lockers are supposed to protect deposited property from theft, natural disasters.[359] Safe deposit boxes would seem an obvious application of the law of bailment, and many courts have held that they are.[360] Operators of safety deposit boxes, usually banks, have argued that they are not in possession of goods stored in safety deposit boxes. One argument that most courts have rejected is that because the bank has no knowledge of what is in the safety deposit box, it is not in possession.[361]

Cloud storage also raises questions about who is in possession of the files that may differentiate it from other kinds of storage. It is almost definitional that cloud storage is available on demand. This means that the person or company that owns the files may be manipulating them perhaps even in possession of them on a local computer while the files live on cloud infrastructure. On these facts, the storage company may be in possession of the files but not strictly exclusive possession.[362]

Some courts have held that bailments only exist where the bailee has "such full and complete possession of it as to exclude, for the time of the bailment, the possession of the owner." Where the owner does not intend to relinquish control, there is no bailment.[363] But cloud storage necessarily involves relinquishing some control. After all, the cloud storage company controls the infrastructure that facilitates the storage. The cloud storage relationship is more than the ephemeral custody of the customer inspecting goods, it is a change in where the goods live.[364] The author concludes by arguing that, despite

[355] Danielle D'Onfro, The New Bailments (Wash. U. in St. Louis Sch. of Law, Working Paper, 2022) (on file with author); Caitlin Dewey, Apple's iMessage Encryption Foils Law Enforcement, Justice Department Complains, WASH. POST (Apr. 5, 2013), https://www.washingtonpost.com/business/technology/apples-imessage-encryption-foils-law-enforcement-justice-department-complains/2013/04/05/f4a6b66e-9d68-11e2-a2db-efc5298a95e1_story.html [https://perma.cc/4VRD-UCTD].

[356] Ibid. 135; Edward J. McAndrew, The Hacked & the Hacker-for-Hire: Lessons from the Yahoo Data Breaches (So Far), Nat'l L. Rev. (May 11, 2018), https://www.natlawreview.com/article/hacked-hacker-hire-lessons-yahoo-data-breaches-so-far.

[357] Ibid. 135; Ryan Vacca, Viewing Virtual Property Ownership Through the Lens of Innovation, 76 Tenn. L. Rev. 33, 51–53 (2008).

[358] Ibid. 135; *Tunkl v. Regents of Univ. of Cal.*, 383 P.2d 441, 446 (Cal. 1963)

[359] Ibid. 129; *Seitz v. Lemay Bank & Tr. Co.*, 959 S.W.2d 458, 464 (Mo. 1998)

[360] Ibid. 129; *Seitz*, 959 S.W.2d at 461

[361] Ibid. 130; *Nat'l Safe Deposit Co. v. Stead*, 95 N.E. 973, 977 (Ill. 1911)

[362] Ibid. 134

[363] Ibid. 134; **Ray A. Brown**, *The Law of Personal Property* § 10.1 (Walter B. Raushenbush ed., 3d ed. 1975).

[364] Ibid. 134

the differences in means of storage due to modern technology, the relationship between the storage company and the client in cloud storage is akin to traditional warehouse storage. Therefore, the author contends that the law of bailment, which governs this relationship, should apply to cloud storage.

However, I would like to disagree with this conclusion of the author and hold that cloud storage is not akin to control and possession of data on two grounds namely,

Cloud storage providers offer a service that goes beyond mere custody of physical items. They provide infrastructure, security, and accessibility features that extend beyond the traditional understanding of a bailee's role. This broader service aspect may warrant a different legal treatment and the relationship between cloud storage providers and users is often governed by detailed contractual agreements, specifying terms of service, data handling, and liability. These contracts may establish a different legal framework than the traditional bailment relationship, emphasizing the importance of voluntary agreements. The grounds of data not screened by the cloud storage company is also a factor that needs to be considered and can be only ascertained after the terms of the agreement.

In essence, while the author draws parallels between safe deposit boxes and cloud storage, I posit that the distinctive nature of the services provided by cloud storage providers, coupled with the intricacies of contractual agreements and data handling practices, necessitates a reconsideration of applying the traditional law of bailment to cloud storage.

Shane Gallant is proposing a concept known as the "adhesion bailment doctrine" as a way to provide greater protection to users of the Internet of Things (IoT) regarding data collection by third-party companies. The idea is based on the notion that, in an IoT world where constant data gathering is prevalent, users are continuously providing data to third-party companies as part of their day-to-day activities. The term "adhesion" is used in this doctrine to emphasize that the information collected is not voluntarily disclosed by the users but is rather a consequence of their routine interactions in the IoT environment.

The argument is that, even though users are continuously providing data, the nature of this collection is not truly voluntary, and therefore, users should maintain their privacy rights in the face of advanced technology and data gathering practices. The doctrine is presented as a response to challenges posed by the third-party doctrine, which traditionally relies on the notion of voluntary disclosure of information by individuals. Shane Gallant has tried to use the adhesion bailment doctrine to safeguard the privacy rights enjoyed by US citizens. The author is trying to point out that once the third parties ie, the IoT companies become bailee of the data they collect, the doctrine would ask them to protect the customers from sharing of their data to the government agency without the concurrence of the said customer and hence would protect privacy rights enjoyed by citizens.

Conclusion:

This paper has tried to address few of the questions of the literature review of the sources on Digital Bailments and its complex application on the principles of the traditional Bailment Doctrine. The paper has tried to address few certainties and application of Digital Bailment doctrine to the Indian context and extrapolate its features on Aadhar Card and its authentication data that needs to be deleted after 6 months and the US position on destroying the data by the private data storage companies and thereby returning to the customer the right (or fact) that they are the sole possessor of the personal data and information.

The paper has further tried to critically analyse the aspect of duty of care in cloud storage and the theory of possession and control of the data. The paper has tried to analyse as to why the authors stand in 'The New Bailments, Danielle D'Onfro, Washington University in St.

Louis School of Law 2022,' can be construed to be incorrect considering the factor that there is screening of data by the cloud storage companies and also there is the stored data can be manipulated by the user to the same extent as one can do in the local drives and hence would be difficult to express the application of bailment theory in the court of law. In Midcon Data Services, LLC v. Ovintiv USA, Inc, 2021, it was held that Midcon may continue to pursue its claim on the alleged destruction of bailment with regards to the physical storage devices defined as the Original Media but may not pursue its claim on the alleged destruction of bailment with regards to the intangible Data. [365] In Krupa v. TIC International Corporation, 2023, the court dismissed the claim of digital bailment for the loss of data that occurred due to hackers stealing the date. The courts in USA are still inconsistent regarding valuing intangible data under traditional Bailment norms.

In conclusion, the paper has tried to find the main issues that are contentious in applying traditional Bailment doctrine to data stored in cloud or in other words called electronic data. Bailment is a relationship between two parties. While it can seem complex with its many categories and formerly convoluted procedural rules, the core is quite simple: bailment is the law of entrusting our things to other people.[366] The way forward is to legislate statutory laws and extend the law of bailment to intangible assets like data and information stored in the cloud as this field will open pandoras boxes in coming future along with privacy laws that are too at stake.

References:

1. **William LaRosa**, *New Legal Problems, Old Legal Solutions: Bailment Theory as the Baseline Data Security Standard of Care Owed to an Opponent's Data in E-Discovery*, 167 U. Pa. L. Rev. 775 (2019), https://www.jstor.org/stable/45389473.
2. **Danielle D'Onfro**, *The New Bailments* (Wash. U. in St. Louis Sch. of Law, Working Paper), donfro@wustl.edu.
3. **Shane Gallant**, *The Old Bailment Doctrine: The Answer to Fourth Amendment Jurisprudence in the Digital Age*, 25 Roger Williams U. L. Rev. 116 (2020).
4. **Richard S. Whitt**, *Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era*, 36 Santa Clara High Tech. L.J. 73 (2019).
5. **Adam J. Levitin**, *Not Your Keys, Not Your Coins: Unpriced Credit Risk in Cryptocurrency*, 101 Tex. L. Rev. 877 (2023).
6. Breach of Bailment of Electronic Data, 91 A.L.R.6th 409 (Originally published in 2014).

Case Laws:

1. *Midcon Data Servs., LLC v. Ovintiv USA, Inc.*, No. CIV-20-1037-SLP, 2021 WL 4923464 (W.D. Okla. Oct. 21, 2021).
2. *Glob. Network Mgmt., Ltd. v. Centurylink Latin Am. Sols., LLC*, No. 1:21-CV-20862, 2023 WL
3. *Krupa v. TIC Int'l Corp.*, No. 22-cv-00733, 2023 WL 143140 (N.D. Ill. Jan. 10, 2023).
4. *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016).
5. *K.S. Puttaswamy v. Union of India,* (2017) 10 SCC 1, 283.

[365] Midcon Data Services, LLC v. Ovintiv USA, Inc, 2021
[366] The New Bailments, Danielle D'Onfro, Washington University in St. Louis School of Law 2022, donfro@wustl.edu. pg 152