VOLUME 6 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

TELECOMMUNICATION IDENTIFIER USER ENTITY (TIUE): PRIVACY, SURVEILLANCE, AND LEGAL ACCOUNTABILITY IN MODERN COMMUNICATIONS

- Shabnam Saleem[1]

Introduction

The surge of digital communication has revolutionized telecommunications as no longer being a strictly technical service, but as a space subject to legal regulation where identity, privacy and accountability collide. Under modern communication systems, user identification is now the focal point of mobile network, internet-based communication systems and the state regulatory systems. All subscribers are usually associated with one or more identifiers, either as a result of a SIM registration procedure, as a mobile number, as a device-based identifier, or account-bound credentials held by a mobile service provider. In this regard, we can think of the term of the Telecommunication Identifier User Entity (TIUE), which can be perceived as the legally and functionally identifiable user of the telecommunications system, whose existence is identified by data points that allow performing authentication, traceability, regulation, and delivery of services. The term as such is not a commonly used legal term, but it summarizes a growing concern of telecommunications law: the legal status of the identity of the user in digitally mediated communications.

TIUE is important because the telecommunication systems would not run in darkness with respect to anonymity. In many instances, current regulatory frameworks provide that the service providers gather, authenticate, store and in certain cases hand over the information associated with subscribers to the government. This legal framework is usually defended based on national

[1] Student (LLM) at Amity Law School, Noida

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/

security reasons, fraud prevention, authorized interception of the law, consumer protection, and market control. Simultaneously, though, legal collection and utilization of telecommunication identifiers also concern some profound issues of privacy, informational autonomy, data protection, and the potential threat of surveillance. This puts the law in a tricky situation: the law needs to allow identifying methods that are needed to conduct legitimate state and business activities and avoid misuse, overreaching, and unwarranted intrusion into the rights of individuals. This strain has now become one of the characteristics of telecommunications regulation in the digital age.[2]

TIUE is most effectively studied not only as a technical issue of network administration, but as a legal issue of the classification, ownership, management, and allowable application of communications-related identity information. A telecommunication identifier can take the form of a neutral one but in reality, it can mention trends of movement, associations, habits of the person and digital behavior. The user party to such identifiers is thus not just a subscriber in the contractual sense, but also a party to the law, whose constitutional, statutory and human rights can be impacted by data collection and access activities.[3] The study of law has come to understand that secrecy is not the sole source of information privacy. Instead, the main question concerns whether the personal information is gathered, processed, and shared beyond the legitimate expectations or is a violation of human dignity, which is particularly acute in the telecommunications sphere since user identifiers tend to operate on a continuous, invisible, and massive scale.

TIUE has become increasingly relevant in the legal context with the introduction of compulsory SIM registration policies, cross border data retention policies, biometric authentication schemes and 4G, 5G and eSIM data systems. These advancements have ensured that user identification is more accurate, unrelenting and valuable to individual players as well as the governments. Meanwhile, they have subjected people to novel types of legal vulnerability, such as identity theft, SIM swap fraud, unlawful profiling, unnecessary data retention, and disproportionate surveillance. There has been a growing demand that judicial and regulatory bodies establish the

[2]Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477 (2006). https://scholarship.law.gwu.edu/faculty_publications/892/

[3]Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* 127–57 (2010). https://www.sup.org/books/title/?id=8862

appropriate boundaries of state and corporate access to communications information.[4] Through the example of Europe, again and again the courts have stressed that traffic and location data can easily disclose highly personal details about personal life, and thus must be subject to a high level of safeguards, access requirements based on necessity, and proportionality.

The reason TIUE should be given special attention in the law study is because it borders with a number of disciplines of law. The telecommunications law deals with licensing, network access, and service-provider requirements; data protection law deals with the gathering and usage of personal data; constitutional and human rights law deals with privacy, dignity, and expression; and criminal law deals with interception, computer-crime, fraud, and the use of communications records as evidence. Consequently, there is no unified legal system that describes the identity of telecommunication users. The meaningful analysis should consequently take an integrated approach. It needs to question, who is in charge of the identifier, and what are some legal obligations surrounding its collection, when, and under what circumstances it can be revealed, and what forms of redress are available in the event of abuse of this kind of information. This is particularly significant in legal frameworks whereby the growth of regulation has preceded the creation of transparency, consent and accountability protections.

This study supports the argument that TIUE is a conceptual metaphor that can be relied upon to analyze how telecommunication legal governance addresses the identification of users. It will allow an organized discussion of how the telecom systems turn people into identifiable entities to be used in operation and regulation and how the law reacts to the ensuing privacy and liability issues. The legal nature and structure of telecommunication user identification will be first discussed in the paper. It will subsequently examine how TIUE impacts privacy, data protection and human rights. Lastly, it will determine the regulatory and liability concerns that emerge due to misuse, unauthorized access and the developing technologies of identification. By doing so, the paper will attempt to show that the future of the telecommunications law is not just centered

[4]Joined Cases C-293/12 & C-594/12, *Digital Rights Ir. Ltd. v. Minister for Commc'ns, Marine & Nat. Res.* and *Kärntner Landesregierung v. Seitlinger*, 2014 E.C.R. I-238. https://curia.europa.eu/juris/liste.jsf?num=C-293/12

on effective identification tools, but also on the creation of protective measures that can maintain the equilibrium between security, regulation, and personal freedom.[5]

Legislative Character and Regulation of Telecommunication User Identification

Telecommunication user identification is legal because it transforms an identifiable individual participant in a communication into a legally recognizable and administratively traceable object in a regulated communications system. In normal technical terms, telecommunication networks are based on identifiers that distinguish users, authenticate access, route communications and serve as service continuity. Those identifiers, however, serve a more profound role in the law. They associate a natural or a juridical person with a set of rights, duties, liabilities and control measures. The subscriber number or SIM registration record or device identifier or account credential or point in the traffic records are not just useful operational data, and they can be transformed into admissible evidence of identity, location, association, and conduct. That is why the telecommunication user identification should be interpreted as the legal institution formed due to the telecommunications regulation, privacy law, data protection law, and principles of public law concerning the state access and procedural fairness.[6]

On the lowest level, the telecommunication user identification structure would start by the legal connection between the subscriber and the service provider. In a legal vacuum, telecommunications service is hardly a reality. It is routinely regulated by licensing systems, legal requirements on operators, contractual relationships between the provider and the customer and regulatory control by national communications regulators. In this design, user identification has a number of applications. It allows activating services, verifying the eligibility of subscribers, facilitating billing and dispute resolutions, eliminating duplication or fraudulent access, and allowing legal compliance with legitimate demands by law enforcement agencies. The user identification is therefore considered as a very fundamental part of the communications governance, but not an appendage of the administration by the legal system. The provider must gather identifying details during subscription and keep records over designated durations in several jurisdictions. This policy is an indication of the belief that access to telecommunications

[5]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119) 1 (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj
[6]Id.

should be associated with a recognizable legal entity that can be held answerable where it is required. However, the same assumption begs the significant questions of proportionality, necessity and the extent of legitimate data collection.

One practical approach to appreciating the legal nature of telecommunication user identification is to differentiate between three layers which are closely related, namely subscriber identity, device-related identity, and communications metadata. Subscriber identity is the personal or corporate data that is used to subscribe to service like name, address, national identity details, or any other verification records. Identity device relates to numbers or identifiers of equipment used within the network such as handset or module identifiers. Communications metadata refers to the information created when using a network, traffic, routing, duration, and location-related details. These categories are analytically different, but they are frequently considered jointly in legal systems since each of the three classes of categories can be used to define a user entity. The law on privacy and data protection in modern days has come to the realization that information that can be used to identify a person or trace him or her cannot be considered to be anonymity just because the information is not a name even in its strictest sense. This is the understanding that is the most vital in the telecommunication in which even without the disclosure of the actual content, patterns of communication can determine personal identity and behavior.[7]

The law that regulates user identification is thus not restricted to telecom specific laws. It is also in effect via the general data protection norms. This legal definition is relevant since under the General Data Protection Regulation of the European Union, any information concerning an identified or identifiable natural person falls within the definition of personal data, a broad term that enforces the lawfulness, fairness, transparency, limitation of scope of purposes, minimization of data, limitation of storage, integrity, and confidentiality concepts upon it.[8] Practically speaking, telecom operators are not allowed by law to collect identifying information in unlimited forms because it may prove handy in the future. They should demonstrate a lawful purpose of processing, relevance and proportionality of the data obtained, safeguard it against abuse and guarantee rights of access, correction and sometimes erase or protest. Thereby the

[7]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, 2002 O.J. (L 201) 37 (Directive on Privacy and Electronic Communications). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0058

[8]Id. art. 4(1).

legal character of telecommunication user identification is both administrative and rights-based: it facilitates the administration of networks, yet only in the context of a system of rights that acknowledges the user as a subject of rights.

The legal framework, together with the data protection law, is influenced by the industry-based privacy regulations on the electronic communications. Under the ePrivacy Directive, additional data protection requirements take the shape of specifications on the privacy of communication, processing of traffic information, and the management of location information in Europe, as the telecommunications poses special risks since the information in the form of the network remains generated at all times.[9] This is in contrast to most other commercial environments where telecom providers are uniquely placed such that they can monitor not just who made a subscription to a service but also when, as well as where and how long, who they talked with. Communications data are sensitive in nature and this has led to a tighter regime in the law. This user identification is not only concerned with the point of entry into the network, but also, it is spread all over the life cycle of the service and also it covers the legal control of the data being created at the point of entry.

The other characteristic of telecommunication user identification is the role of the state. Governments usually present subscriber identification regimes under the pretext of national security, prevention of crime, enforcing anti-terrorism, and preventing fraud. A notable example is the mandatory SIM registration laws. These laws mandate that users must have identity documentation in view before accessing or even enabling mobile service thus linking access to a legally verifiable identity. Regulatively, such laws have been justified as measures to enhance accountability and help to investigate crimes. Regarding their rights aspect, they are however controversial as they normalize traceability and can even be used to instigate mass surveillance or discrimination. The law should then seek to answer the question of whether or not they should be identified in this manner, whether more less intrusive methods are available and the provisions to ensure that the identity is not abused. European courts have made it very clear through judicial rulings that the data belonging to communications retention and access cannot be handled like any other administrative issue when the retained data may reveal any intimate

[9]Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557 (2004).

details of personal life. The Court of Justice of the European Union in Digital Rights Ireland concluded that indiscriminate retention of electronic communications data amounted to a severe encroachment on fundamental rights, especially since the traffic and the location data could give detailed inferences about personal life, habits, and social relations.[10]

This is a jurisprudence that is vital in determining the legal framework surrounding telecommunication user identification. It indicates that law does not consider telecom identifiers as neutral infrastructure. Rather, identifiers are perceived to be gateways to a larger informational space which can reveal personality, association, and autonomy. There are legal implications. To begin with, any user identification framework should meet the standard of legality i.e. the gathering and utilization of identifying information should be expressly allowed by the legislation. Second, it has to meet the requirement of necessity and proportionality, i.e. the severity of identification should be reasonable by a valid purpose and should be limited to the strictly necessary. Third, proper protection should be in place in regard to access, storage, control, and correctives. In the absence of these safeguards, telecom identification schemes will be used as a tool of excessive surveillance instead of a legitimate regulation measure.

The framework is also explained by the doctrinal literature on privacy. The taxonomy of privacy by Solove proves that privacy harms are not just the result of information being published by a provider of a number, file of subscribers, or similar information.[11] The damage may start way before, when the data is systematically gathered, integrated across systems, or stored unnecessarily. Another valuable theoretical contribution is made by Nissenbaum theory of contextual integrity, that information flows are not lawful or unlawful due to content alone, but due to whether they comply with proper social and institutional standards.[12] In telecommunications, users may agree that network functionality requires certain kinds of identification data to be processed by the service provide, but they may not reasonably expect that such data will be shared with third parties, stored indefinitely or The point of view supports the notion that the identification of telecommunication users should be evaluated contextually and normatively, rather than operationally.

[10]Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev. 1375 (2004).
[11]Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. Ill. L. Rev. 1417
[12]Supra note 9

The scheme of telecommunication user identification can thus be viewed as a mixed legal regime. It is contractual since it is a development of the subscriber provider relationship. It is regulatory in the sense that communications authorities require identification, record keeping and compliance responsibilities. It is constitutional and human-rights grounded since intrusive identification interferes with privacy, dignity, expression, and freedom of association. It is also evidence-based and liability-focused since identifiers are frequently referred to in fraud investigations, criminal prosecutions, civil litigations, and regulation enforcement. This is the reason why telecommunication user identification cannot be simplified to a technical task of labeling users. It is a legal procedure that makes people visible to networks, corporations and states.

To sum it up, the legal telecommunication user identification is based on its dualism, i.e., it is both a service administrative mechanism and a locus of legal power. It enables the providers to authenticate users and provide communications effectively, yet the technology also opens routes to monitoring, control, and accountability. The regulatory framework is informed by telecommunications regulation, data protection regulations, electronic communications privacy law, and principles of proportionality and protection of rights by the judiciary. Any serious legal discourse of TIUE shall then be concerned not merely with how users are identified, but with the legal boundaries, protections and institutional obligations which regulate that identification. It is only at that point that the law can strike the right balance between regulation requirement and personal freedom.

Privacy, Data Protection, and Human Rights Concerns

The problem of human rights, privacy, and data protection takes a center stage in the legal analysis of telecommunication user identification. When a telecommunications system, based on subscriber records or device-linked identifiers, traffic metadata, or location information identifies a user, then that user is no longer just a member of a technical network. The user turns into a recognizable legal entity and the data concerning communications might be gathered, archived, processed, disseminated, and even revealed to the state. This revolution has significant legal implications since the telecommunications data is especially sensitive. Although the content of communication may not be accessed, the information regarding, who communicated, when,

where and the duration of communication may reveal the secrets concerning personal life, social life, movement, political affiliation, health issues and professional activity. It is due to this that privacy in the telecommunications law should be construed to have gone beyond secrecy of content to encompass privacy besides excessive identification and unnecessary retention and unwarranted access to information connected to communications.[13]

The very possibility to gather telecommunication identifiers is the first area of law. Telecom operators will frequently cite network security, billing, fraud control and regulatory pressure as reasons to impose identification requirements. These intentions might be just, yet, the gathering of the information related to identity is not unrestricted legally. The principles of data protection stipulate that processing of personal data should be both lawful and fair and sensible.[14] The legal implications of this broad definition under General Data Protection Regulation, personal data is any information that relates to an identified or identifiable natural person, which obviously means the telecom operators have to find a relevant legal basis to process the information, collect only the necessary data to serve a specific purpose, and provide adequate security measures. The law thus declares the perception that service providers can collect all the identifiable information just because technological systems enable it to be collected. It instead stipulates that the practices of identification must be warranted by a valid purpose and be limited by the principles of necessity and proportionality.

A second important issue is related to data retention. Metadata is frequently produced by the telecommunications systems in the course of normal network operation, and in most jurisdictions regulatory regimes have sought to have providers maintain such data in order to be available at the request of law enforcement or national security. Legal controversy in this case is considerable since retained traffic and location data may expose in-depth patterns of individual life despite the fact that the content of messages may not have been read. The Court of Justice of the European Union tackled that matter with great vigor in Digital Rights Ireland and argued that indiscriminate retention of electronic communications data amounted to a severe intrusion of the fundamental rights to privacy and data protection. This argument is specifically applicable to the

[13]Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681 (2011).
[14]Neil M. Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 Wash. U. L. Rev. 1441 (2017)

identification of telecommunication users as it substantiates that identifiers and other metadata are not to be considered as nothing other than technical or administrative. They are sensitive to law due to inferences that they allow. Therefore, blanket retention regimes present deep human rights issues other than limited and with effective safeguards.[15]

Privacy in telecommunication is also strongly intertwined with the concept of confidentiality of communications. The law of communications sector-specific acknowledges that privacy in this case should not be applied in the content alone, but also to the information on traffic and location produced by the use of the networks. This is the rationale of the ePrivacy Directive in the European Union; to ensure confidentiality of communications and to restrict the situations when traffic data can be processed or stored. They are in a position to see current communication patterns as part of the service unlike many other data controllers.[16] Devoid of stringent legal restrictions, the daily running of networks might turn into an instrument of continuous surveillance and profiling. Privacy law is therefore a structural curb against commercial exploitation as well as State overreach in the public sector.

Telecommunication identification is even more evident with concerns on human rights when it is associated with surveillance and access by the state. Governments often claim that the investigation of serious crime, terrorism, cyber threats, and fraud needs access to subscriber identity and communications metadata. These are usually considered as valid in the law of the land. But legality is not sufficient as the doctrine of human rights demands. Any violation of privacy should be law prescriptive, have a legitimate purpose, and be necessary in a democratic society. The European Court of Human Rights has on numerous occasions emphasized that surveillance practice should be furnished with sufficient and efficient protection against abuse and more so when there are secret spy powers at stake. The court determined in Roman Zakharov v. Russia that a system of surveillance without adequate protection infringed the right to respect to private life under Article 8 of the European Convention on Human rights.[17] The relevance of that decision to the telecommunications law is that the overreach of surveillance systems was not only dangerous, but also incompatible with the rule of law. The identification of

[15]Id.
[16]Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934 (2013).
[17]*Roman Zakharov v. Russia*, App. No. 47143/06, Eur. Ct. H.R. (Grand Chamber) (Dec. 4, 2015).

telecommunication users whether in conjunction with extensive surveillance authority can thus freeze free expression, deter association and destroy trust in communication infrastructure.

The other aspect of the issue is the informational autonomy and dignity. Privacy theorists have maintained that the damage of spying and acquiring data is not necessarily tied to the street revelation of humiliating truths. The influential taxonomy by Daniel Solove demonstrates that any of the following harms arising when no dramatic disclosure involves collection, aggregation, secondary use, insecurity and exclusion may be caused by privacy harms. A user will never learn when the identifying information about him or her is pooled across systems, stored beyond any useful use, disclosed to third parties, or accessed by the authorities. However, all these practices are potentially autonomy-destroying because they deny one of control over the flow and interpretation of information about them. The theory of contextual integrity by Helen Nissenbaum supports this fact as it suggests that privacy is maintained when information flows are appropriately regulated by social norm within a certain context.[7] When people agree that a telecommunications operator may scan their data to make and accept a call or to maintain the quality of services, they did not agree to be profiled to unrelated purposes, indefinitely, and in an unlimited manner. The legal issue is not, however, whether there is data, but whether the terms of its flow are both normative and legally warranted.

Equality and exclusion are also an issue in telecommunication user identification. The system of mandatory identification skews the burden on disadvantaged groups, which are not formally documented, do not have addresses, and do not have access to government-provided identity documents.[18] Where this happens, telecom identification is not simply a method of control over the already established users, it can also be a gatekeeping process that leaves vulnerable individuals out of the much-needed communication services. The accessibility of telecommunications in the contemporary digital landscape is directly linked to the ability to be engaged in education, employment, medical services, financial services and civic life. Strict identification framework can thus influence not just the rights to privacy but also equality, non-discrimination as well as social inclusion. The issue is more acute when biometric verification or centralized digital identity frameworks are brought into place lacking proper safeguards,

[18]Julie E. Cohen, *What Privacy Is For*, 126 Harv. L. Rev. 1904 (2013).

transparency, and available corrective measures in case of error. False identifications, inappropriate deactivation, or errors in the databases can deny people access to communication and leave them with few sources of judicial recourse.

Moreover, identity theft and data leakage prove that telecommunication user identification is rather dangerous both in private law and in the public law. Service providers that receive identity documents, numbers, addresses, and records that are related to networks place solemn security and confidentiality duties. Without obtaining such data, a user can be exposed to fraud, SIM swap attack, impersonation, financial loss, or reputation damage. Data protection law also enforces obligations pertaining to integrity and confidentiality, whereas tort, consumer and contractual doctrines may offer a supplementary solution in certain legal frameworks. The significance of these requirements is hard to overestimate. The more robust the identification system, the more harmful the impacts of the compromise. Data security should thus be analyzed as part of the human rights and privacy framework, as opposed to being an accidental technical consideration.

Finally, the issue of privacy, data protection, and human rights indicates that the identification of telecommunication users is not a matter of law. It works on the border of legitimacy regulation and possible overreach. Identification has the potential to aid in prevention of fraud, integrity of services and legal investigation, but can also aid in profiling, surveillance, exclusion and abuse when not limited enough. The legislation should thus demand explicit statutory authority, restrictive collection, retention necessitated, formidable security, separable control, and viable remedies. It is only through the integration of telecommunication identification into a rights-affirming paradigm that the legal systems can justify the needs of the order and technological growth against the principles of dignity, liberty, and personal autonomy.

Regulatory and Liability Issues in Telecommunication Identification

Identification of telecommunication users has some of the hardest legal issues in the modern communications law since it makes the law to not only establish who may be identified, but also who is liable when the identification systems are misused, compromised or applied in a manner that infringes individual rights. Telecommunication identification is not merely a network administration issue in the realm of law. It is a regulatory process by which states, service

providers and users are put in a complied, accountable, and possible liability relationship. The relationship has found its place especially amid the regime of compulsory SIM registration, digital onboarding, eSIM activation, biometric verification, cross-border, and state overreliance on communications data to police and national security. The legal question of whether telecommunication user identification must take any form at all is however not the core of the matter, but rather the capacity of regulators to establish the scope of lawful telecommunication user identification, and to make the operators and the government accountable in terms of abuse, negligence, and unreasonable interruption of rights.[19]

A significant area of regulation regards the commitments of the telecommunications service providers. There are many legal requirements that providers verify the identity of subscribers, keep proper records, safeguard communications data, and comply with lawful requests of regulatory and investigative agencies. Such responsibilities are brought about by licensing terms, communications statutes in the sector, anti-fraud regulations, consumer-protection statutes, and data-protection laws. The provider, thereby, fulfills a dual role: he is a commercial actor, who is involved with customers, as well as a controlled mediator, who has responsibility to the populace. This legal position creates a high standard of care. In a system where a provider has not verified identity appropriately, permitted activation with false documents, failed to provide security measures, or otherwise revealed subscriber data unlawfully, it can face regulatory penalties, civil liability or in certain systems even criminal penalties. The judicial system thus considers telecommunication identification as one of the fields whereby the private players play a quasi-public role and should be subjected to increased expectations of diligence.[20]

This dual logic of regulation is reflected in the problem of SIM registration. Some states demand that users provide identification documentation prior to gaining mobile access on the basis that these steps will help prevent fraud, enhance traceability and give law enforcement a means to track down serious crime. Regulatively, this places a legal obligation on the providers to gather and store the identifying information at the entry point into the communications system. But the liability risks are also created by the imposition of such duties. When records are erroneous,

[19]Supra note 3

[20]Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247 (2011).

falsely prepared, or carelessly stored then the identity regime can not serve its claimed purpose and at the same time will expose users to damage. A provider who switches on a SIM on fake credentials e.g. may allow criminal use and later accuse an innocent user whose identity has been stolen or duplicated. Under these conditions, the liability issue cannot be considered exclusively in terms of the actions of the user. It also has to answer the question of whether or not the operator complied with its legal duty of verification and whether or not regulatory control was robust enough.

Another regulatory issue is the retention and disclosure of subscriber/traffic related data. Service providers might have to hold information to enable billing, enforce a contract, resolve a dispute, and in certain jurisdictions, access by law-enforcement. Nonetheless, courts have become more aware of the fact that a wide-ranging or discriminatory retention duty is a menace to core rights.[21] The legal merit of this argument is that blanket retention of electronic communications data was a severe encroachment on privacy and data protection due to the volumes of personal inferences such data might allow. The liability issue is both institutional and personal where the legislation requires too much retention or has weak protection against access. Different authorities may have the duty to introduce rules that are rights-incompatible, and the third party (that is, the provider) may accept liability in case of data processing or disclosure that is not authorized by the law.

State access is an important issue that should be considered in regulatory responsibility. Telecommunications law usually authorizes the disclosure of subscriber data or metadata by court order, statutory warrants, or legal interception systems. But the presence of legal authority does not preclude the issue of liability. Jurisprudence of the European Court of Human Rights has placed a strong emphasis on the need to ensure that secret surveillance powers has sufficient safeguards against abuse, such as by limiting the extent, authorization by some body, oversight and providing effective sanctions. The Court in Roman Zakharov v. Russia established that a surveillance regime that did not provide adequate protection violated Article 8 of the European Convention on Human Rights.[22]As to telecommunication identification systems, this principle implies that it is a concern not only to design but also to the implementation. A provider that

[21]Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. Ill. L. Rev. 1417.
[22]Supra note 16

allows a technical operation access to user information without heed to verification, or a state that allows a wide access without any substantial control, can facilitate a violation of rights even when the system is publicly introduced as legal. Regulatory frameworks have to deal not solely with authorization in theory, but also with institutions being accountable in practice.

The liability is also concerned with data breaches and security failures. The more the detail identification system, the more damage that can be caused when it is put to the test. Identity information Subscriber identity records, associated phone numbers, account credentials, location histories, and device identifiers are desirable by criminals committing identity theft, SIM swap fraud, financial fraud, extortion, and social engineering. In the data-protection law, operators must take the necessary technical and organizational measures to ensure that personal data is not subjected to unauthorized access, loss, or disclosure.[23] This principle is reflected in the General Data Protection Regulation through obligations of integrity and confidentiality and breach-notification obligations in relevant instances. Here, the liability is not only retributive, but it has a preventative role by encouraging more robust security governance and internal control mechanisms.

Another important regulatory issue is intermediary accountability. In the case of user identification data, telecom operators are not mere conduits as such. They proactively gather, validate, store, organize and occasionally transfer this information. This makes them stand out of actors who passively perform content without identity processing. Legal frameworks are therefore able to place affirmative compliance obligations pertaining to customer due diligence, record quality, retention restrictions, auditability and collaboration with governmental bodies. These responsibilities should however be well balanced.[24] When operators are transformed into vigilante enforcement agencies, it can lead to the over-collection, over-retention and routine disclosure of personal information. In case, however, operators are not properly regulated, user rights can be insufficiently secured. The law thus has a calibration issue: there must be specifications of responsibilities so that accountability is attained, but there must be restraint against incentives to overly or defensively process data.

[23]Supra note 4

[24]Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 Harv. L. Rev. 2010 (2013)

The balance is aggravated by emerging technologies. The transition to a 5G architecture, cloud-controlled services, eSIM provisioning, and the incorporation of integrated systems of digital identity increase the number of participants in the identification process. This means that the identity of the user can now be created, authenticated, stored and shared at various levels, which include telecom providers, platform operators, identity verification vendors, and cloud infrastructure services. This disintegration causes legal ambiguity over control, shared responsibility and jurisdiction. In case of an error during identification, when data is moved across the boundaries, or the wrongdoer inflicts harm upon a user due to a breached onboarding system, it can be complicated to tell which party is liable to legal action. The law of data protection has tried to answer some of these questions by introducing the concept of controller, processor and joint controllership, but on the telecom ecosystem, their application remains complicated.

Liability is also given a significant dimension by human rights law. States must not merely avoid illegal interference; in most cases they should introduce the legal systems that would guard individuals against being abused by the non-state actors as well. Even in a situation in which telecom identification systems place their users at risk of surveillance, fraud, exclusion, or discrimination, insufficient regulation can be a human rights problem by itself. This is more so in instances where people do not have a proper solution to wrongful deactivation of SIM cards, mis-identification, and unauthorized leakage or lockout of communication services because of some failures in documentation. The rule of law is all about access to a remedy. A regulatory mechanism that develops traceability, but lacks a system of correction, review, compensation, and appeal is at risk of being unilateral and coercive.

The law of telecommunication identification in terms of doctrine can thus be viewed as a branch of layered liability. First, operators could be liable of careless verification, unlawful disclosure, inadequate security, or failure to compose data-protection duties. Second, the responsibility of disproportional retention laws, an abusive surveillance system, or the absence of procedural protections may be placed on the public authorities. Third, users can bear civil or criminal responsibility provided in situations in which they use false identities, commit fraudulent registration or misuse another individual telecommunication credentials. However, these

liabilities ought not to be taken as isolated by a well crafted legal framework. It must divide the responsibility in a way that is reflective of institutional power, its technical aptitude, and real control over the data flows.

To sum up, telecommunication identification regulatory and liability aspects indicate that TIUE is not only a hypothetical apparatus of identifying users but a legal framework where authority is decentralized and responsibility is imposed. The telecommunication identification systems can contribute to lawful governance goals, including security, fraud, and effective service delivery, but it opens doorways towards irresponsibility, abuse, and breach of rights. The legislation should thus control this area by having clear legal mandates, specific duties of providers, high security levels, autonomous control, and easy redress. It is only in this context that the telecommunication identification can be compatible with the larger values of legality, proportionality, and human dignity.

Conclusion and Recommendations

The legal discussion of Telecommunication Identifier User Entity (TIUE) reveals that the telecommunication user identification is much more than a technical process of connecting a subscriber to a communication service. It is a legal process by which people are identified, controlled, supervised, and in certain instances, exposed to both social and private evils. As demonstrated in the preceding discussion, telecommunication identification is in the interface between telecommunications regulation, privacy law, data protection law and human rights law. It has justifiable uses such as network management, fraud prevention, lawful access, customer authentication and service delivery. Simultaneously, though, it raises grave legal issues where collection, retention, disclosure or use of identifying data is more than necessary and proportional in a democratic legal order. The idea of TIUE is hence applicable since it aids in the conceptualization of telecom identity as not only working data, but legal relationship between the user, the service provider, and the state.

One of the major findings of this paper is that telecommunication identifiers must be treated as legally sensitive information. SIM registration information, traffic information, location information, subscriber records and information associated with the device might all be used to identify an individual. In places where the content of messages is not read, these types of data

can create very revealing conclusions about the habits, movements, associations, and personal life of a person. That is why the modern legal systems, especially in the European paradigm, do not consider communications metadata as something insignificant and technical any more. Rather, both the law and case law have acknowledged over time that user identification data should be regulated by lawfulness, fairness, necessity, proportionality, and accountability.[25]The fact that telecommunication identifiers are personal data implies that telecom operators cannot process the data in arbitrary ways. They should ensure they have a reason to process, should only collect the data when it has a legitimate purpose, guard against the misuse of the data, and should have procedural safeguards where the disclosure to the public authorities is part of the process.

The second big conclusion is that the legal system that regulates the identification of telecommunication users is still divided. User identification is touched upon by telecom law, data protection law, law on surveillance, consumer law, the doctrine of constitutional rights, but none of the regimes completely solves the conflicts between them. The law on telecommunications commonly places an emphasis on efficiency, traceability, and regulatory compliance. The law of data protection emphasizes minimization, transparency and privileges of the user. The human rights law is concerned with the privacy, dignity and safeguarding against the unjustified intrusion of the state. In practice such structures can be at odds, or disproportionate, particularly in legal systems where the rate of technological development is faster than in legal change.[26] This fragmentation exacerbates the fact that telecom identification systems have grown in practice and administrative convenience, as opposed to a more legality-limited and constituted legal approach, where the governance of telecommunication identifiers is not subjected to a limited industry approach, but to a wider constitutional and rights-based approach.

The paper also demonstrates that the lawful operation of telecommunication identification system focuses on the regulatory and liability issues. Service providers hold a rather special role since they are both private actors and mediators regulated. They have the responsibility of gathering and storing user identity information, ensuring communications-related information is safe, and address legal regulatory or investigative requests. This is a serious responsibility. In situations where providers do not ensure identification in an appropriate manner, store or transfer

[25]Supra note 10
[26]Supra note 20

subscriber information in a careless manner or enable disproportionate access by state actors without proper protections, liability can be imposed under data protection law, regulated enforcement systems and, in certain systems, civil or criminal law. Similarly, it is true that, the public authorities can be held liable when they establish or sustain surveillance and retention regimes that are unnecessarily broad, under-supervised, or inappropriate in relation to fundamental rights.[27]The law should therefore provide that responsibility be distributed in accordance with factual power and control over telecommunications data, and not disproportionately devolved on individual users.

The other important conclusion is that telecommunication identification is not just restricted to the issue of privacy. Comprising mandatory identification systems can establish access obstacles to undocumented individuals, marginalized populations, and individuals who do not possess formal credentials, which service providers or state systems recognize. On the same note, fraud of money, SIM swap attacks, image damage, and denial of necessary communication services are only some of the ways individuals can be victims of data breaches and identity misuse. The access to telecommunications in the contemporary world is greatly linked to the engagement in education, employment, health, trade, and civic living. Therefore, user identification misuse or overregulation does not only influence privacy but also equality, autonomy and social inclusion. The legal regulations of TIUE should then be sensitive to both distributive concerns and liberty-based concerns. A secure non-invasive or efficient rights-invasive telecom identification system cannot be considered legally satisfactory.

Based on these findings, it can be proposed that there are a few recommendations. First, the scope and use of telecommunication user identifiers should have a more definite statutory definition. The types of data that can be gathered, the purpose of gathering them, the authority to gather data, and the duration of the gathered data should be specified in the laws. Loosely defined or unrealistically broad clauses must not be used as they provide room to stretch the law and cause inconsistent application. Second, there should be intensified data minimization, accuracy and security requirements on telecom operators. Only the user identity data necessary to fulfill pre-defined legal and operational aims needs to be collected and well-established

[27]Ira S. Rubinstein, Ronald D. Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. Chi. L. Rev. 261 (2008).

technical and organizational barriers must be implemented to avert unauthorized access or misuse.[28]

Third, telecommunication identification data should be accessible to the public authorities based on the necessity procedures, independent authorization, and substantial supervision. The blanket or indiscriminate retention regime must not be accepted and preferably narrowed down to rules that are at least consistent with proportionality and judicial review. Fourth, remedies to instances where the telecommunications identification systems cause harm to the users should be readily available. These resolutions ought to entail rights of access, correction, complaint, review, and compensation where necessary. Law responsibility should be pragmatic, rather than formal. Fifth, new technologies like eSIM, integration of digital identity, cloud-controlled telecom services, and cross-border data processing need to be regulated by the telecommunication industry in the future. Such trends make classic paradigms of control and responsibility complicated and it is necessary to define the position of the controllers, processors, and shared responsibility in telecom ecosystems.[29]

To sum up, TIUE can be useful in terms of an analytical approach to the systems of law in telecommunication identity in the digital era. It embodies the fact that telecom users are not just merely attached to networks but are rather named, categorized and regulated with both legal and technical frameworks that define their rights and vulnerability. The future of the telecommunications law will be determined by the ability of legal systems to maintain the operational advantages of user identification without using it to become an instrument of excessive surveillance, exclusion, or abuse. A rights-respecting framework should thus hold that telecommunication identification should be pegged on a legal, proportionate, accountable, and human dignity platform. It is only in this manner that the law can balance fairness in terms of security, regulatory efficiency and preserving the freedom of the individual.

References

Articles and Books

[28]Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183 (2016).
[29]Andrew Keane Woods, *Against Data Exceptionalism*, 68 Stan. L. Rev. 729 (2016).

1. Bamberger, Kenneth A. & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 **Stan. L. Rev.** 247 (2011).https://www.stanfordlawreview.org/print/article/privacy-on-the-books-and-on-the-ground/
2. Balkin, Jack M., *Information Fiduciaries and the First Amendment*, 49 **U.C. Davis L. Rev.** 1183 (2016). Link: https://lawreview.law.ucdavis.edu/issues/49/4/Articles/49-4_Balkin.pdf
3. Bellia, Patricia L., *Surveillance Law Through Cyberlaw's Lens*, 72 **Geo. Wash. L. Rev.** 1375 (2004).
4. Cohen, Julie E., *What Privacy Is For*, 126 **Harv. L. Rev.** 1904 (2013). Link: https://harvardlawreview.org/print/vol-126/what-privacy-is-for/
5. Freiwald, Susan, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 **Md. L. Rev.** 681 (2011).
6. Mulligan, Deirdre K., *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 **Geo. Wash. L. Rev.** 1557 (2004).
7. Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* 127–57 (2010).https://www.sup.org/books/title/?id=8862
8. Ohm, Paul, *The Rise and Fall of Invasive ISP Surveillance*, 2009 **U. Ill. L. Rev.** 1417.
9. Richards, Neil M., *The Dangers of Surveillance*, 126 **Harv. L. Rev.** 1934 (2013).
10. Richards, Neil M., *The Third-Party Doctrine and the Future of the Cloud*, 94 **Wash. U. L. Rev.** 1441 (2017).
11. Rubinstein, Ira S., Ronald D. Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 **U. Chi. L. Rev.** 261 (2008).
12. Solove, Daniel J., *A Taxonomy of Privacy*, 154 **U. Pa. L. Rev.** 477 (2006). Link: https://scholarship.law.gwu.edu/faculty_publications/892/
13. Strahilevitz, Lior Jacob, *Toward a Positive Theory of Privacy Law*, 126 **Harv. L. Rev.** 2010 (2013).
14. Woods, Andrew Keane, *Against Data Exceptionalism*, 68 **Stan. L. Rev.** 729 (2016).

Cases

15. Joined Cases C-293/12 & C-594/12, *Digital Rights Ir. Ltd. v. Minister for Commc'ns, Marine & Nat. Res.* and *Kärntner Landesregierung v. Seitlinger*, 2014 E.C.R. I-238.https://curia.europa.eu/juris/liste.jsf?num=C-293/12

16. *Roman Zakharov v. Russia*, App. No. 47143/06, Eur. Ct. H.R. (Grand Chamber) (Dec. 4, 2015).

Legislation

17. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, 2002 O.J. (L 201) 37 (Directive on Privacy and Electronic Communications). Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0058

18. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016, 2016 O.J. (L 119) 1 (General Data Protection Regulation). Link: https://eur-lex.europa.eu/eli/reg/2016/679/oj