Use of Digital Evidence In Psychological Assessments and Its Forensic Interpretation

Dr. Anjali Yadav[1], Saumya Solanki[2]
[1]*Assistant Director & Scientist 'C', Central Forensic Science Laboratory (CFSL), DFSS, MHA, New Delhi, India*
[2]*Forensic Professional, Central Forensic Science Laboratory (CFSL), DFSS, MHA, New Delhi, India*

Abstract: **Digital evidence can strengthen the case of a forensic psychologist provided it is appropriately obtained, forensically maintained, and contextualized for the interpretation. Social media is a complete, date-stamped history of behavior, communication and interpersonal relationship that forensic psychologists employ as collateral information in forensic evaluations. Social media provides a rich, time-stamped archive of an individual's behavior, social interactions, and communication. It also serves as a supplemental resource in answering questions regarding risk, intent, credibility, functional capacity, and personality during interviews and tests. Social media aids in testing and interviews but has to be dealt with forensically, ethically and with explicit statements of limitation. However, social media evidence must be treated with the appropriate forensic and ethical guidelines, and a degree of uncertainty must be articulated in a social media evaluation.**

Keywords: **Digital Evidence, Forensic Psychologist, social media.**

I. INTRODUCTION

Digital evidence can also strengthen forensic psychological assessment case when it is used strategically, conservatively, and openly. Digital evidence refers to data that is created, stored, or transmitted using electronic devices and networks. It is central to contemporary investigations and, adjudications, and for a good reason. Because it is temporally precise, behaviorally rich and ubiquitous, it can attest to an event in a powerful manner that is hard to contest. Therefore, it is not surprising that it can be considered the "best evidence" for most investigation, if present.

Digital entities have timestamps, location information and event histories that are capable of generating action sequences with granularity unavailable from human memory or bodily traces. Social media timelines, chat histories and device use create continuous traces of behavior that indicate pattern, escalation and stability over time. Use metrics, sensor data and metadata generate quantifiable surrogates for sleep, activity, mobility and communication to complement subjective report. Digital footprints continually link people, networks and third parties across jurisdictions and platforms, illustrating coordination and linkage unseen by legacy evidence. Much digital evidence is contemporaneous documents (email, system logs, CCTV reports) generated independently of subsequent testimony and reduce dependence on faulty human memory. While digital evidences can be employed to corroborate Forensic assessment but the forensic psychologist will have to keep in mind that the information may be faked, edited, spoofed or taken out of context; user submitted captures and screenshots are particularly vulnerable without metadata and forensic confirmation. Digital evidence are a powerful addition to forensic psychological practice if they are collected lawfully, preserved forensically, and interpreted in context.

Though digital evidences are there to strengthen the Forensic assessment but the forensic psychologist must consider that the data can be fabricated, edited, spoofed or taken out of context; screenshots and user- submitted captures are especially vulnerable without metadata and forensic verification. Posts, memes and messages often use irony, role performance or platform- specific norms; literal readings can mislead. Device ownership and

attribution problems: Presence of data on a device does not automatically prove who authored or controlled it at a critical moment. Not all demographics leave the same digital trace; absence of evidence on a platform may reflect access, preference or censorship rather than innocence. Encrypted data, server side records and cross border data stewardship create access hurdles and evidentiary.

II. HUMAN BEHAVIOR AND DIGITAL EVIDENCES

The Digital evidences can offer rich insights into an individual's psychological makeup and behavioral tendencies. The following aspects illustrate how different forms of digital evidence can reflect underlying human behavior.

- Trait indicators: posting frequency, social network size, and language use correlate with Big Five dimensions.
- Affective style: posting diurnal rhythms, emoticon use, and sentiment patterns indicate baseline mood variation as well as affective reactivity.
- Impulse control and risk taking: late evening mobility, spontaneous location moves, and seeking of risky activities can index impulsivity and sensation seeking.
- Aggression and interpersonal style: aggressive assertions, rejection/withdrawal patterns, or conflict threads running throughout indicate aggression, hostility, or instability in relations.
- Cognitive style and openness: novelty-seeking ideas and linguistic complexity, diversity of content define openness and intellectual curiosity.
- Values and identity signals: profile self-presentations, group membership and selected photos reflect identity priorities, ideological commitment, and moral signaling.
- Stability and consistency: longitudinal traces (months to years) enable testing whether behaviors witnessed are stable characteristics or temporary states.

This perspective shows how digital evidence, when interpreted carefully, can offer a meaningful window into human behavior

III. METHODOLOGY FOR PERSONALITY RESEARCH FROM DIGITAL TRACES

To understand personality through digital footprints, researchers combine computational techniques with behavioral science principles. The methods below outline how different data streams are analyzed to infer psychological characteristics:

- Language analysis: lexical and syntactic characteristics, topic modeling and time series/sentiment analyses to project language indicators onto characteristics.
- Behavioral time series: activity rhythms sleep surrogates, regularity of mobility and response latencies in order to infer routine, conscientiousness and social interaction.
- Network analysis: ego network measures (centrality, density) to quantify social influence and connectedness.
- Content coding: coded or manual themes (aggression, self disclosure, pro social posts) to measure value orientations and interpersonal.
- Multimodal fusion: integration of text, images, Meta data and sensor data provides a more comprehensive personality profile than any single channel.
- Validation: correlate digital measures with tested personality inventories and collateral reports to demonstrate local reliability.

Forensic Psychology takes account of variation with respect to platform norms (Instagram Vs LinkedIn) and can prefer performance of role rather than trait. Online traces by online activity are subject to influence by age, socioeconomic status and digital literacy. Lexical indicators are per-formative or ironic; beginner sentiment scores misinterpret subtlety. Crisis bias affects short-term crises; longitudinal data are needed for claims of traits. Bots, ghosting, multiple accounts and faked content can misrepresent perceived personality.

How computer evidence enhances assessment: Computer evidences aids in rebuilding accurate timelines and situational precipitants. They verify or invalidate self report and collateral history. Aids in identifying acute risk markers (overt threat, means

seeking, accelerated escalation), provides objective functional markers (pattern of activities, social functioning) and signals discrepancies indicative of malingering or memory failures that require evaluation.

IV. CONCLUSION

Digital evidence substantially enhances what forensic psychologists are able to see, document, and understand about human behavior. It delivers ecological, real-time, and multi-layered knowledge that standard assessment methods alone cannot supply. However, how carefully and properly these facts are incorporated into practice determines how beneficial they are. Meaningful conclusions require clearly framed questions, sound analytic procedures, adherence to psychometric principles, and strict attention to legal and ethical safeguards.

Future progress in this field will rely on developing culturally sensitive coding approaches, strengthening validation across multiple data modalities, and training practitioners to interpret metadata and digital patterns with accuracy and caution. Establishing shared standards that balance evidentiary strength with privacy and fairness is equally essential. When applied with care, digital evidence does not replace clinical judgment—it enhances it, supporting more informed, scientifically grounded, and ethically responsible forensic assessments.

REFERENCES

[1] Arshad M, Ahmad A, Onn CW and Sam EA (2025) Investigating methods for forensic analysis of social media data to support criminal investigations. Front. Comput. Sci. 7:1566513. doi: 10.3389/fcomp.2025.1566513

[2] Ashley B. Batastini, Michael J. Vitacco, 978-3-030-33907-4, Forensic Mental Health Evaluations in the Digital Age, Published: 25 February 2020

[3] Ayush Sood, Shubhani Aggarwal , Shobhita Singh NFSU – Journal of Cyber Security and Digital Forensics, ANALYSIS OF DIGITAL FORENSIC PRACTICES IN INDIA Volume –3, Issue – 1, June 2024 E – ISSN – 2583-7559

[4] Harshit Gupta, Prof. (Dr.) Monika Rastogi and Ruchi Kaushik, The Intersection of Digital Forensics and Criminal Investigation in India: Legal and Procedural Dimensions of Evidentiary Standard, 4 IJHRLR 127-144 (2025). Available at www.humanrightlawreview.in/archives/.

[5] Prof. (Dr.) Radhika Dev Verma2, Role of Digital Forensics and Criminal Investigation in India Deepali1, International Journal of Research Publication and Reviews, Vol 5, no 11, pp 87-94 November 2024.