PROTECTING CLIENT-LAWYER CONFIDENTIALITY DURING VIDEO CONFERENCING IN COURT

OPINION REPORT

BY PAUL MUKIIBI

JUNE 2025

Background:

The digitization of judicial proceedings has led to the widespread adoption of virtual court hearings in Uganda and beyond. While remote court appearances have improved access to justice and reduced logistical burdens, they have also introduced new challenges, particularly in safeguarding the fundamental right to client-lawyer confidentiality. This issue is especially critical for incarcerated individuals who attend court proceedings from correctional facilities via video conferencing platforms.

Traditionally, advocates and their clients have had the opportunity to consult in private before or during court sessions. However, in virtual court environments, especially when the accused appears from a prison facility, these private interactions are often compromised. Prisoners may not have access to a secure, confidential communication channel with their lawyers. Attempts to consult during proceedings whether by speaking aloud or gesturing can be overheard, recorded, or intercepted by unauthorized third parties. This undermines legal professional privilege.

The lack of confidential communication channels can also hinder effective legal representation, limit the ability of advocates to receive timely instructions, and expose sensitive information to potential misuse.

Uganda's judiciary and correctional services must now consider implementing similar safeguards to ensure that the transition to digital justice does not erode the rights of the accused.

This calls for a careful examination of existing technologies, legal obligations, and administrative processes to facilitate confidential, secure, and effective communication between advocates and their clients during virtual court sessions.

SOME OF THE JURISPRUDENCE PROHIBITING TAPPING CLIENT-ADVOCATE CONVERSATIONS

Lanza v. New York (370 U.S. 139 (1962)

The Supreme Court explained that *"[e]ven in a jail, or perhaps especially there, the relationships which the law has endowed with particularized confidentiality must continue to receive unceasing protection."*
The Ninth Circuit Court of Appeals elaborated on this when it said: *[I]t takes no stretch of the imagination to see how an inmate would be reluctant to confide in his lawyer about the facts of the crime, perhaps other crimes, possible plea bargains, and the intimate details of his own life, and his family members' lives if he knows that a guard is going to be privy to them, too.*

United States v. Black, U.S.D.C. (D. Kan.), Case No. 2:16-cr-20032-JAR.

A Special Master David R. Cohen filed a request with the U.S. District Court in Kansas, seeking to enlarge his investigation into whether the Leavenworth Detention Center (LDC) and the private contractor that operates the facility, had improperly recorded privileged attorney-client meetings and shared those recordings with federal prosecutors.
As a result, on August 10, 2016 a Kansas federal district court ordered the practice to "cease and desist" immediately. U.S. District Court Judge Julie A. Robinson also ordered that all originals and copies of such recordings be surrendered immediately to the court.
Judge Robinson's order left no doubt of her position on the matter. She ordered *"all detention facilities in Kansas and Missouri, as well as CCA, that house detainees charged in this district, to immediately cease and desist all: (1) audio-visual recording of attorney-client communications in the detention facility; (2) audio recording of attorney-client phone calls; and (3) audio-visual recording of attorney-client videoconference calls."*

Source: https://www.prisonlegalnews.org/news/2016/oct/3/judge-orders-end-recording-attorney-client-meetings-ccas-leavenworth-detention-center/

PRACTICAL SOLUTIONS

01

Implementation of Virtual Breakout Rooms for Private Consultation

Modern video conferencing platforms such as **Zoom, Microsoft Teams, and Cisco Webex** offer features that can replicate the in-person experience of stepping aside for a confidential consultation. Specifically, breakout rooms can be configured as secure virtual spaces within the main courtroom session.

Before the hearing begins, the court administrator or judicial clerk can designate a breakout room labeled "Advocate–Client Consultation." Access to this virtual room is restricted by invitation, allowing only the defense counsel and the accused to enter. Once inside, the room operates as an isolated channel where no other participant judges, prosecution, prison officers, or registry staff can monitor or intercept the conversation.

The breakout room must leverage the platform's native encryption protocols **(e.g., Zoom's AES 256-bit GCM encryption or Webex's TLS 1.2 with Advanced Encryption Standard)** to secure both video and audio streams. If required, courts can enforce **end-to-end encryption (E2EE)** to eliminate even server-side access, ensuring no data passes through unencrypted intermediaries.

This model facilitates confidential consultations before the hearing commences, during a pause, or even after the hearing, depending on the judicial officer's discretion. Administrative staff should be trained to monitor entry logs (not content) for scheduling and audit purposes without compromising the sanctity of the communication.

02 Deployment of Dedicated Lawyer–Client Video Booths Within Correctional Facilities

Correctional institutions should establish designated legal consultation booths equipped with secure, tamper-proof video conferencing hardware. These booths must be architecturally and technologically designed to uphold confidentiality.

Technically, each booth should include:

Sound-Insulated Physical Enclosure

The booth must be constructed using acoustic panels or composite soundproofing materials to eliminate audio leakage. The design should meet ***Class A acoustic privacy standards, ensuring voices cannot be heard outside.***

Noise-Cancelling Headsets

Each user (the incarcerated person and the advocate, if physically present) must be equipped with digital noise-cancelling headsets using active noise control (ANC). This prevents ambient noise from being transmitted and reduces the chance of hidden recording devices picking up sound within the booth.

Secure Video Terminal with Encrypted Connectivity

A wall-mounted tablet or industrial-grade terminal should run a locked-down operating system **(e.g., hardened Android or Linux-based OS).** This terminal must connect only to a judicially authorized video conferencing platform, such as a **private instance of Zoom for Government or Jitsi** Meet configured with end-to-end encryption.

The device should be connected to a dedicated **VLAN (Virtual Local Area Network),** physically and logically segmented from the prison's main network. Access must be gated via a firewall with intrusion detection/prevention systems (IDS/IPS) and updated SSL/TLS encryption protocols.

Automatic Activation of an Anti-Tapping Countermeasure System

Once the consultation session is initiated, the booth should automatically engage an active anti-surveillance system, such as:

- *Near-Field Acoustic Masking (NFAM) Generator.* This is a white-noise emitter that projects ultrasonic or low-frequency masking signals that interfere with the microphones of covert recording devices (including mobile phones, wearable recorders, or pinhole microphones).

- *RF Signal Scrambler / Detector.* The booth should have a real-time RF spectrum scanner that detects unauthorized radio frequency transmissions (2G–5G, Wi-Fi, Bluetooth, etc.). If illicit surveillance signals are detected, the system logs the event and may activate a narrowband signal jammer (within legal prison-use limits) to suppress eavesdropping transmissions.
- *Faraday Shielding.* The booth structure can be partially wrapped in EMI (Electromagnetic Interference) shielding material to prevent external electromagnetic access to the audio or video signals. This turns the booth into a mini Faraday cage, significantly increasing protection from remote tapping or device hijacking.

The video communication channel must be encrypted using Transport Layer Security (TLS) or E2EE protocols, preventing network sniffing or interception by unauthorized users.

Correctional officers may maintain line-of-sight supervision (as a security precaution), but they must remain outside the audio range during ongoing legal consultations. Surveillance audio equipment should be explicitly disabled or omitted for these booths, except in instances where a judicial order permits monitoring due to compelling security threats.

03 Integration of Secure Parallel Communication Channels Using Encrypted Messaging Apps

Where permissible, lawyers and clients may agree to use end-to-end encrypted messaging applications to communicate in parallel to the courtroom video session.

Apps such as **Signal, Threema, or WhatsApp** (with disappearing messages enabled) allow secure, real-time side discussions.

The mobile devices used should meet the following minimum technical standards:

- A jail-issued or court-permitted locked-down tablet or phone configured with access only to pre-approved apps and contacts.
- The messaging app must support asymmetric cryptography (e.g., Signal uses the Signal Protocol, which employs **Curve25519, AES-256, and HMAC-SHA256).**
- Device and app data should be ephemeral, using features such as disappearing messages and biometric lock to prevent unauthorized post-session access.

United Kingdom Benchmark: Preserving Lawyer–Client Confidentiality in Remote Hearings via Prison Video Link (PVL)

The United Kingdom offers a mature and procedurally secure framework for safeguarding legal professional privilege (LPP) in remote legal proceedings involving prisoners. Central to this is the Prison Video Link (PVL) system a standard facility across Her Majesty's Prisons that enables detainees to attend court hearings, consultations, and bail applications via secure audiovisual links.

A key aspect of the PVL framework is its recognition of the inviolability of lawyer–client confidentiality. The Ministry of Justice (MoJ), through its official guidance on PVL requests, provides for dedicated "legal conference" sessions that allow confidential discussions between counsel and prisoner either before or after the court session. These sessions are scheduled independently of the main court hearing and are designed specifically to uphold **Article 6 of the European Convention on Human Rights**, guaranteeing the right to a fair trial, including access to legal counsel without interference.

In some jurisdictions and courts, particularly those using the Cloud Video Platform (CVP), additional confidentiality measures are built into the platform itself. These include the use of headphones or earphones to mitigate the risk of unintended auditory disclosure and, in certain courtrooms, private chat functions or parallel audio breakout rooms to facilitate side conversations between advocates and their clients during the hearing.

The Law Society of England and Wales has provided clear normative guidance emphasizing that **"video hearings must include mechanisms for private communication with clients to preserve legal professional privilege"** (Law Society, 2020). This professional imperative echoes the position of the Bar Council, which asserts unequivocally that *"[e]veryone must have the right to consult with their lawyer in private. Prisoners should not be treated as exceptions to that rule"* (Bar Council, 2021).

Moreover, recent commentary from civil society organizations such as the Prison Reform Trust and Fair Trials has affirmed the need for reforms and best practices that include privacy-preserving digital legal access. Their reports call for PVL implementation to guarantee non-monitored access to lawyers, the ability to speak confidentially, and the availability of digital channels to replace or supplement in-person consultations where necessary (Prison Reform Trust, 2022).

Together, these measures position the United Kingdom as a best-practice jurisdiction in the digital justice space. Its layered safeguards legal, procedural, and technological ensure that even within the constraints of incarceration and remote hearings, attorney–client confidentiality remains protected, consistent with both domestic constitutional guarantees and international human rights obligations.

REFERENCES

GOV.UK (2023). Request a Prison Video Link. Ministry of Justice.
Available at: https://www.gov.uk/guidance/request-a-prison-video-link

Law Society of England and Wales (2020). Access to Justice in the Remote Court Era.
Available at: https://www.lawsociety.org.uk/topics/research/access-to-justice-in-the-remote-court-era

Bar Council (2021). Legal Professional Privilege for Prisoners.
Available at: https://www.barcouncil.org.uk/resource/legal-professional-privilege-for-prisoners.html

Prison Reform Trust (2022). Screening Out Justice: The Impact of Remote Courts on Access to Justice.
Available at: https://www.prisonreformtrust.org.uk/publication/screening-out-justice/

Fair Trials (2021). Justice Under Lockdown.
Available at: https://www.fairtrials.org/publication/justice-under-lockdown/