

Safe Communications for Remote *Ex Parte* Protective Order Hearings

Courts, law enforcement agencies, and domestic violence service providers that are partnering to offer remote *ex parte* protective order hearings or to expedite service of protective orders all need to be aware of Internet security and the protection of documents that travel back and forth among them.

Protective Order Confidentiality

Rule 7, ARPOP—Public access to case information

For as long as a plaintiff has the ability by law to have a protective order served or unless otherwise ordered by the court, the court must not make publicly available any information regarding the filing for, contents of a petition for, or issuance of a protective order until proof of service of the protective order has been filed with the court. The court may share information about the protective order with the plaintiff, prosecutors, or law enforcement.

Rule 123(d)(3), Rules of the Supreme Court—Protective Orders.

For as long as a plaintiff has the ability by law to have a protective order served or unless otherwise ordered by the court, the custodian shall not make publicly available any information regarding the filing of or contents of a petition for or issuance of a protective order until proof of service of the protective order has been filed with the court. The custodian may permit law enforcement agencies to access these records when necessary to carry out their official responsibilities.

Rule 7, Arizona Rules of Protective Order Procedure, and Rule 123, Rules of the Supreme Court, each require that protective orders be kept confidential and out of public view until the order has been served on the defendant. When courts, law enforcement agencies, and domestic violence service providers team up to make remote *ex parte* hearings or expedited service possible, both Internet and document security need to be considered so that the court rules are followed.

This is **basic** information about Internet and document protection. Each partner should confer with its own IT professionals regarding available methods for ensuring security of its communications on the Internet or encrypting or password protecting documents that move back and forth during the process.

- Use a proprietary network. Ideally, video hearings should be conducted through a network controlled by government agencies (for example, a court and a police department).
- Use a virtual private network (VPN) to conduct a video hearing. If one of the partners is not a government agency, the non-government partner should consult with the court about installation of VPN software on a specific computer at the non-government partner's location. The computer on which the VPN software installed should be used only for the purpose of conducting video *ex parte*



hearings with the court. VPN is a locked connection that encrypts and decrypts the information that is traveling between the partners.

- An unprotected wireless network within the non-government partner's facility also poses risk. A wireless network can be protected by MAC (media access control) authentication. This restricts the wireless access point to accept traffic only from devices having their unique identifier registered before use. Consult an IT professional for advice on protecting a wireless network. (Connecting the computer directly to the router using a cable eliminates the wireless risk, provided that the computer's wireless facility is turned off.)
- Encrypt or password protect documents. Software or ZIP utilities are available that can encrypt files. The recipient of the encrypted file must have a program that can decrypt the protected document. The password or encryption key that is needed to open the document must be sent separately (in another email, by text message, or instant message, for example). Never send the password or key to a password-protected or encrypted document in the email to which the document is attached.
- Provide a link to the files from within Microsoft OneDrive. The "government cloud" OneDrive storage area used by courts and some local governments is encrypted and requires an ID and password for outside access. Providing a user with read-only access keeps the document under your control and prevents downloading or re-sharing.
- Use a file-synchronization service only as a last resort and only when all partners agree that this method is adequately secure. Dropbox is an example of a file-sync service that works with a shareable link. Password protect the files before placing them in the shared location. Never send the password in the same mail as the link to the documents. Confirm with your IT professional that the file-sync service is actually encrypting shared files.

