E-DISCOVERY

REQUESTING PARTIES MUST UP THEIR GAME IN CYBERSECURITY.

WRITTEN BY **CRAIG BALL**

PROTECTIVE ORDERS ARE frequently used to enable litigants to designate information produced in discovery as "confidential." This is a useful tool to ensure that discovery isn't used for competitive intelligence. With a protective order in place, lawyers, experts, and support personnel can access sensitive information while ensuring the information won't be misused. Proponents of protective orders characterize them as routine safeguards to be accepted without question by parties seeking discovery. "We require these in all our cases" may be the only rationale offered in support.

Over time, protective orders have evolved to include stringent obligations to protect information produced in discovery. Similarly, e-discovery production protocols often impose cybersecurity and privacy protection duties.

Keen to proceed with discovery, counsel all too often execute these orders and protocols giving little consideration to how they will honor the many commitments they impose or whether their firms are equipped to meet the demands of providing the requisite protection.

Cybersecurity and personal privacy are real and compelling concerns. Just about everyone has been victimized by a data breach, and lawyers are tempting targets for hackers because lawyers and law firms hold petabytes of sensitive and confidential data. Firms slow to adapt to changing times and emerging threats are easy prey for data thieves.

Corporations are demanding that outside counsel implement exacting data protection protocols and do more than pay lip service to protecting, e.g., personally identifiable information, or PII; protected health information, or PHI; privileged information; and, above all, information lending support to those who would sue the company for malfeasance or regulators who would impose fines or penalties.

Additionally, corporate clients are making outside counsel undergo security audits and institute operational and technical measures to protect confidential information. These measures include encryption in transit and at rest, two-factor authentication, access controls, extensive physical security, incident response capabilities, cyber liability insurance, federal and international (e.g. ISO) certifications, and compulsory breach reporting.[1]

Forcing outside counsel to harden their data bulwarks is important and overdue. It's also disruptive and costly. Some firms will find it more difficult to compete. Savvier firms will embrace cybersecurity and frame it as a market differentiator.

And in litigation, outside counsel will necessarily seek to impose comparable duties on to counsel for requesting parties any time "confidential" information is produced.

Ultimately, all lawyers must up their game in protecting sensitive data, but until that happens, requesting parties, experts, and litigation support providers will find themselves grossly unprepared to supply the rigorous cybersecurity and privacy protections made a condition of e-discovery. That incapability will be asserted as a basis to deflect and defer discovery.

Requesting parties may be tempted to respond by fighting demands for rigorous data protection, arguing that such protections weren't sought in times past. Fighting to be cavalier about data security is a battle that requesting parties cannot win and should not fight. Requesting parties must instead be ready to put genuine protections in place and articulate them when challenged.

A protective order isn't the answer if it's an empty promise. Requesting parties can't agree to employ rigorous data protection and then go about business as usual: e-mailing confidential data, storing it on unencrypted media, and failing to ensure that all who receive confidential data from counsel handle it with requisite caution. Agreeing to be bound by protective orders and production protocols without the ability or the intention to meet the obligations of the order is a trap. High-profile gaffes will follow, and the failure of a few will be the undoing of many as isolated failures are trotted out as a basis to bar production to all.

Requesting parties cannot expect to be held to a lesser standard of cybersecurity than the producing parties compelled to surrender confidential data to them. A veteran trial lawyer once observed, "Defendants are forgiven several lies. Plaintiffs get none." A party can be careless with its own data because it's theirs, but counsel who fail to protect an opposing party's confidential data will be harshly judged. They don't just hurt their clients and opponents—they undermine the very foundations of discovery.

What must counsel for requesting parties do? Here are a dozen suggestions:

1. Take cybersecurity duties seriously. It's not someone else's job. It's your job. You are the gatekeeper. This is rule one not by accident.
2. Don't just treat an opponent's confidential data with the care you afford your own; treat it better. It's like money in your trust account. You don't treat client monies/data like your own. You don't commingle client monies/data with yours, and you don't use that money/data for anything but permissible purposes with careful record keeping.
3. If there's a protective order, read it closely and be sure you fully understand what it obliges you to do in terms of the day-to-day

conduct of anyone who accesses confidential information.

4. A proper chain of custody is essential. You must be ready to establish who received confidential data and the justification for its disclosure. You must be able to prove you had a good faith basis to believe that the person receiving confidential data understood the need to protect the data and possessed the resources, training, and skill to do so. This obligation encompasses anyone who gets the data from you, including experts, clerical staff, associated counsel, and service providers. Anyone with access to confidential data must be well-prepared to protect the data because their failure is your failure.
5. Proceed with caution when disclosing confidential data to experts. Don't supply confidential data to an expert without first obtaining the expert's consent to receive and protect it. People who appreciate the burden of protecting other people's sensitive data want to hold as little of it as possible. Importantly, because industry experts serve multiple masters and may seek to exploit confidential data obtained in one matter in other engagements, secure the expert's written commitment not to do so and enforce it.
6. Remember that the other side designates what parts of their production must be afforded special protection. Their designation triggers your duty. If you think something isn't properly designated as confidential or sensitive, challenge the designation; but, until the other side agrees or the court sustains your challenge, the designation controls.
7. Confidential data should be encrypted in transit and at rest. This means that none of the confidential data gets attached to an email, moved to portable media like a thumb drive, or uploaded to the cloud *unless it is encrypted*. No exceptions. No excuses. And if you store or transmit the decryption keys alongside the encrypted data, it doesn't count as encrypted.
8. Perimeter protection isn't enough. The biggest risks to confidential data are internal threats, that is, from a craven or careless member of your own team. *Trust but verify*. Access to confidential data should be afforded only on an as-needed/when-needed basis.
9. Access to confidential data must be monitored and logged, as feasible. Remote access and after-hours access should be audited. Safeguard the other side's confidential data in much the same manner as banks protect the contents of safe deposit boxes: There is physical security (walls, doors, alarm systems, and guards) and monitoring of the perimeter (cameras and key cards). There's a vault to keep all contents safe when the perimeter is breached and access controls to make contents available only to authorized persons (dual-keyed boxes and ID/signature scrutiny). Data protection also incorporates elements of perimeter security (limiting physical access to the devices and systems), monitoring (logging and auditing), a vault (strong encryption with sound key management), and access controls (two-factor log in credentials and user privilege management).
10. Have a written data security and incident response policy and protocol in place and *conform your practice to it*. Be sure all employees with access to sensitive and confidential data agree to be bound by the policy, and train everyone in proper cybersecurity. You must first recognize a risk to be prepared to meet it. "No one told me to do that" is not the testimony you want to hear when your staff members take the stand.
11. Be wary of oppressive obligations to destroy or "return" data when a case concludes. Confidential case data tends to seep into mail servers, litigation databases, document management tools, and backup systems. Are you prepared to shut down your firm's email and destroy its backup media because you failed to consider what an obligation to eradicate data would really entail? Have you budgeted for the cost of eradication and certification when the case concludes?
12. Consider cloud-based storage and review tools that integrate encryption, two-factor authentication, and access logging. The cloud's key advantage lies in a user's ability to shift many of the physical and operational burdens of cybersecurity to a third party. It's not a complete solution, but it serves to put a secure environment for confidential data within reach of firms of all sizes.

If this sounds like a big, costly pain, you're paying attention. It's a headache. It slows you down, and the risks grow and change as fast as the technology. But if requesting parties don't put adequate protections in place on their own, courts will allow producing parties to dictate what hoops requesting parties must jump through to obtain discovery—if, indeed, courts don't deem the risk so disproportionate that they deny access altogether.

Discovery is hard enough. Don't make it harder by giving opponents the ability to claim you can't be trusted to protect their information. **TBJ**

NOTES

1. For an example of emerging standards, *see* the Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information promulgated by the Association of Corporate Counsel, https://www.acc.com/sites/default/files/resources/advocacy/1454057_1.pdf.

CRAIG BALL
is an adjunct professor at the University of Texas School of Law and at Tulane Law School, teaching electronic evidence and digital discovery. He is an expert in digital forensics, emerging technologies, visual persuasion, electronic discovery, and trial tactics, limiting his practice to service as a court-appointed special master in electronically stored information. A founder of the Georgetown University Law Center E-Discovery Training Academy, he serves on the academy's faculty. An energetic speaker at continuing legal education programs for the bench and the bar throughout the world, Ball is also an instructor in computer forensics and electronic evidence to multiple law enforcement and security agencies. His articles frequently appear in the national media. For nine years, Ball wrote the award-winning column on computer forensics and e-discovery for *American Lawyer Media* called "Ball in your Court," and still pens a popular blog of the same name at ballinyourcourt.com. He is the 2019 recipient of the State Bar of Texas Gene Cavin Award for Lifetime Achievement in Continuing Education.