

NEW JERSEY LAWYER

August 2022

No. 337

PRIVACY

Treat Your Data Breach Investigation Like Your Toothbrush—Don't Share it with Anyone

PAGE 12

Legislative Approaches to Use of Biometric Information in Society: What it Means for Businesses

PAGE 16



The true north for accuracy and dependability for over 110 years.



Since 1911, Charles Jones has been the pioneer in accurate, dependable public record searches. With solutions that mitigate risk and increase peace of mind, Charles Jones continues to lead the way in accuracy and reliability. To learn more, visit charlesjones.com or call 800-792-8888.

Embracing the past. Navigating the future.

Charles Jones
A DataTrace Company



Scan to view our solutions and services.

© 2018-2022 Charles Jones LLC and/or its affiliates. All rights reserved.

LAWPAY[®]

AN AFFINIPAY SOLUTION

+



Member
Benefit
Provider

"I love LawPay! I'm not sure why I waited so long to get it set up."

— Law Firm in Ohio

Trusted by 50,000 law firms, LawPay is a simple, secure solution that allows you to easily accept credit and eCheck payments online, in person, or through your favorite practice management tools.



22% increase in cash flow with online payments



Vetted and approved by all 50 state bars, 70+ local and specialty bars, the ABA, and the ALA



62% of bills sent online are paid in 24 hours

**PAYMENT
RECEIVED**



YOUR FIRM
LOGO HERE

Trust Payment
IOLTA Deposit

New Case Reference

**** * 9995 ***

TOTAL: \$1,500.00

VISA



POWERED BY
LAWPAY

eCheck

DISCOVER

PAY ATTORNEY

Get started at
lawpay.com/njsba
855-504-7190

Data based on an average of firm accounts receivables increases using online billing solutions.

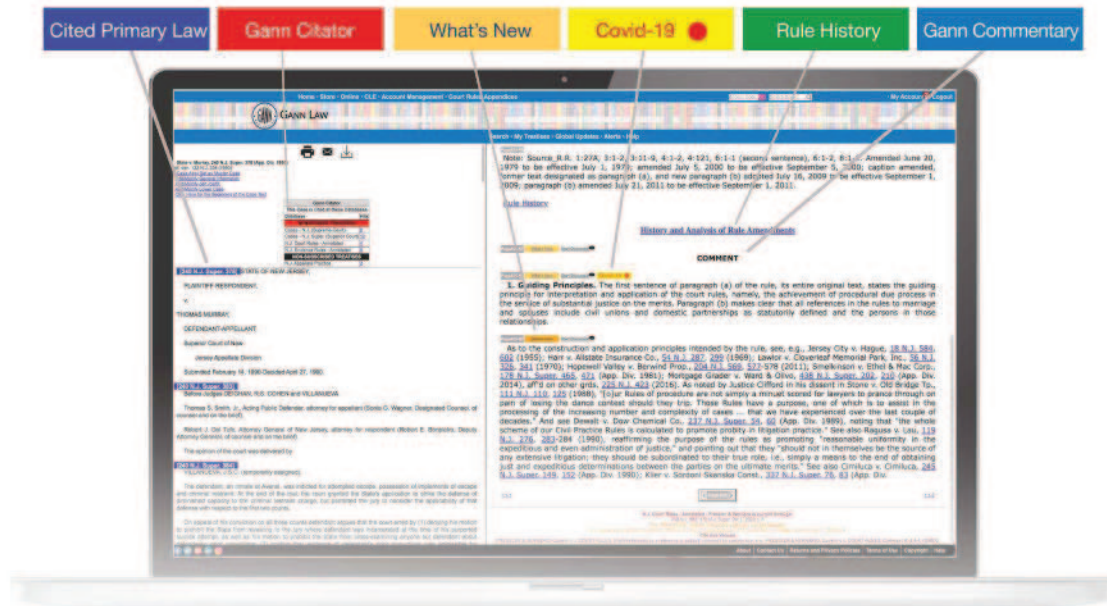
LawPay is a registered agent of Wells Fargo Bank N.A., Concord, CA, Synovus Bank, Columbus, GA, and Fifth Third Bank, N.A., Cincinnati, OH.



GANN TREATISES ONLINE

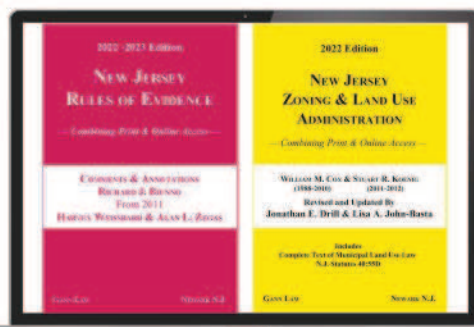
GET MORE DONE, FASTER

SAVE 20%* ON GANN TREATISES ONLINE



Access our Online Only Store by scanning the
QR Code: **NJLM (password)**

Learn How Gann Online Can Save You Time:
www.gannlaw.com/training



Essential Titles Published This Year

- NJ Criminal Code - Title 2C - Annotated
- NJ Arrest, Search & Seizure
- NJ Child Custody, Protection & Support
- NJ Court Rules - Annotated
(2023 Edition to be available in September)

Gann Law • Web www.gannlaw.com • Email sales@gannlaw.com • Phone (973) 268-1200
Fax (973) 268-1330 • Mail 550 Broad Street - Suite 906 - Newark, NJ 07102

* Offer expires 10/1/22 • Online Only Treatises are priced 20% less than the Print+Online Editions

NEW JERSEY LAWYER

August 2022

No. 337



© ISTOCKPHOTO

In this Issue: **Privacy**

Treat Your Data Breach Investigation Like Your
Toothbrush—Don't Share It with Anyone 12

By Daniel J. DeFiglio

Defining Privacy of Biometric Information: Legislative
Approaches to Growing Use of Biometrics in Our Society
and What it Means for Businesses. 16

By Brett R. Harris and Natalie Moszczynski

What Every In-House Attorney Should Know About
Preserving the Confidentiality of Forensic Reports Related
to a Security Incident 22

By Angelo A. Stio III, Avrohom C. Einhorn, and Brianna M. Alunni

Retaining Privacy with Non-Waiver Orders 28

By Veronica J. Finkelstein

Continued



Page
16



Page
22



Page
28

Continued from page 3

Coordinating Care: Aligning 42 CFR Part 2
with HIPAA 33
By David N. Crapo

Commercialization of Your DNA: Privacy Regulations
Lagging for Companies Collecting Genetic Data..... 38
By Jayla E. Harvey

Dragging Dark Patterns into the Light: Recognizing and
Mitigating the Pervasive Risk of Manipulative Interface
Design for Clients in the Digital World 42
By Alfred R. Brunetti

DEPARTMENTS

President’s Perspective..... 5
Message From the Special Editors 6
Practice Tips..... 8



Page
33



Page
38

PRESIDENT'S PERSPECTIVE

JERALYN L. LAWRENCE

Task Force Working Toward Positive Change for Lawyers



When I was installed as president of the New Jersey State Bar Association I announced the creation of the Putting Lawyers First Task Force. Today, I am here to report that it is already hard at work.

The task force is made up of over 30 attorneys from a wide arrange of practice areas, including criminal, civil, family, as well as attorneys who practice at large, mid-size and solo firms around the state. This summer they rolled up their sleeves to start looking for real, concrete, and meaningful ways to make the practice better for all of us.

The task force will spend the next several months examining issues that are impacting our colleagues, leading to stress, anxiety, and depression. It won't simply collect a list of complaints, rather it aims to propose steps that will lead to positive change.

The task force will examine several topics, including:

- How to improve lawyers' ability to attend to mental health and physical health issues.
- Studying how the ethics system works, such as fee arbitrations, character review process and disbarment issues, with an eye toward offering constructive suggestions.
- Looking closely at how malpractice cases play out, specifically examining whether there are recommendations to be made related to affidavits of merit coming from practicing attorneys in the same area as the person who is charged with committing malpractice, similar to the requirements

for medical malpractice actions.

- An examination of how attorneys can ethically protect their online reputation, as it has become more and more common for clients to leave reviews on websites.
- A detailed review of the law surrounding how attorneys can appropriately be relieved as counsel and similarly how they can be assured of fair compensation for their work on a matter.
- Provide recommendations to help solo and small-firm attorneys and new attorneys address the financial aspects of running a firm ethically, as well as how to balance and juggle family responsibilities.
- Study the practice of using initials in certain family law case rather than names to determine if there are alternative best practices to employ.
- How the legal community can work together to ensure the Court's mediation and arbitration programs are utilized effectively and have the resources needed to yield the best results when cases are sent along that path.

To tackle this work, the task force will dig into data, reports, gather information via surveys and collect input from meetings with key officials around the legal community. The goal is to create a comprehensive report that will be submitted to the NJSBA Board of Trustees to consider and implement.

Now, I ask for your help and feedback.

We all know there are many great aspects of practicing law and that there are challenges, too. Tell us about what you love and what issues we can drill in on. Share your experiences in the profession, what works well, what you think needs to be addressed and how we can work together to effectuate change.

Send me an email with your insights at askthenjsba@njsba.com. ■

STAFF

Angela C. Scheck	Publisher
Mindy Drexel	Managing Editor
Janet Gallo	Creative Director
Lynn Marie Gallo	Advertising

EDITORIAL BOARD

Asaad K. Siddiqi	Chair and What I Wish I Knew Editor
Rita Ann M. Aquilio	Vice Chair
Senwan Akhtar	
Lori Ann Buza	
Eric C. Cohen	Ethics and Professional Responsibility Editor
John C. Connell	
Nancy Del Pizzo	Writer's Corner Editor
Angela Foster	Tech Tips Editor
Bonnie C. Frost	
Darren Gelber	
Philip W. Lamparello	
Brian R. Lehrer	A View from the Bench Editor
Dawn M. Monsen Lamparello	
Susan L. Nardone	Working Well Co-Editor
Mary Frances Palisano	
Brian G. Paul	
Michael J. Plata	
Michael F. Schaff	Practice Perfect Editor
William S. Singer	
Lisa J. Trembly	
Albertina Webb	Working Well Co-Editor
Brandon L. Wolff	

NJSBA EXECUTIVE COMMITTEE

Jeralyn L. Lawrence	President
Timothy F. McGoughran	President-Elect
William H. Mergner Jr.	First Vice President
Christine A. Amalfe	Second Vice President
Norberto A. Garcia	Treasurer
G. Glennon Troublefield	Secretary
Domenick Carmagnola	Immediate Past President

New Jersey Lawyer (ISSN-0195-0983) is published six times per year. Permit number 380-680. • Subscription is included in dues to members of the New Jersey State Bar Association (\$10.50); those ineligible for NJSBA membership may subscribe at \$60 per year. There is a charge of \$2.50 per copy for providing copies of individual articles. • Published by the New Jersey State Bar Association, New Jersey Law Center, One Constitution Square, New Brunswick, New Jersey 08901-1520. • Periodicals postage paid at New Brunswick, New Jersey 08901 and at additional mailing offices. POSTMASTER: Send address changes to New Jersey Lawyer, New Jersey State Bar Association, New Jersey Law Center, One Constitution Square, New Brunswick, New Jersey 08901-1520. • Copyright ©2022 New Jersey State Bar Association. All rights reserved. Any copying of material herein, in whole or in part, and by any means without written permission is prohibited. Requests for such permission should be sent to New Jersey Lawyer, New Jersey State Bar Association, New Jersey Law Center, One Constitution Square, New Brunswick, New Jersey 08901-1520. • New Jersey Lawyer invites contributions of articles or other items. Views and opinions expressed herein are not to be taken as official expressions of the New Jersey State Bar Association or the author's law firm or employer unless so stated. Publication of any articles herein does not necessarily imply endorsement in any way of the views expressed or legal advice. • Printed in U.S.A. • Official Headquarters: New Jersey Lawyer, New Jersey State Bar Association, New Jersey Law Center, One Constitution Square, New Brunswick, New Jersey 08901-1520. 732-249-5000 • Advertising Display 732-565-7560.

FROM THE SPECIAL EDITOR

Navigating the Upside Down in the Real World of Privacy

By Nancy A. Del Pizzo

Privacy. It is one word that touches voluminous areas of legal practice. And while it may remind us of science fiction concepts, it is live and functioning in the real world. It also is one of the least static areas of law. In other words, lawyers who



practice in the privacy space cannot relax and rely on past year's authority. That is where this issue of *New Jersey Lawyer* steps in. Here, 10 of your colleagues address critical issues and concerns and recent decisions in the privacy space with valuable practice tips.

First up is Daniel J. DeFiglio's article, "Treat Your Data Breach Investigation

Like Your Toothbrush: Don't Share It With Anyone." It is a title that means what it says: For those of you beginning to or embroiled in helping clients investigate data breach incidents and forming the required and most appropriate response, this article is a must-read. Also featured in this issue is a thorough and unique overview of the use of biometric information and implications for business. Brett R. Harris and Natalie Moszczynski help us understand how biometric identifiers are being used and not just recent laws addressing that use but also proposals for regulations, collec-



NANCY A. DEL PIZZO is a Partner at Rivkin Radler LLP and based in the firm's Hackensack office. Her practice primarily involves litigation and transactional intellectual property issues, including advising clients on privacy concerns.

tions, usage and storage of this valuable personal information.

In the following pages, you also will have the opportunity to read an article from Angelo A. Stio, Avrohom C. Einhorn and Brianna M. Alunni discussing what in-house attorneys need to know about preserving the confidentiality of forensic reporting efforts to address security incidents. There are potential privacy pitfalls when engaging a forensic consultant to aid in a security incident investigation, but Stio, Einhorn and Alunni provide guidance for how companies can preserve confidentiality. Maintaining confidentiality is also the focus of Veronica Finkelstein's piece on non-

waiver orders and how to use them when a case requires voluminous discovery. Her useful tips are paramount to protecting privileges when undertaking e-discovery efforts.

For those in the health care space, or interested in learning more in that space, David N. Crapo addresses how to align 42 CFR Part 2 with HIPAA regulations. Specifically, his article addresses the nuances between regulations focused on persons challenged with substance abuse and privacy laws governing health care generally.

Rounding out this issue are two important works addressing some of the most challenging issues in the privacy

space. Jayla E. Harvey presents an important piece on the commercialization of deoxyribonucleic acid (also known as DNA), discussing emerging privacy issues related to collection of genetic data. And, while Alfred R. Brunetti's ominous title, "Dragging 'Dark Patterns' Into The Light...," connotes the popular Netflix series *Stranger Things*, there is no science fiction here. His article will amaze and inform as it addresses the purposeful manipulation in the interface designs of mobile applications, websites and social media platforms related to user personal information and how to appreciate associated legal risks.

We hope you enjoy this issue! ■

NJSBA CAREERHQ

The New Jersey State Bar Association, the state's largest organization of judges, lawyers and other legal professionals, is the go-to source for finding your next career opportunity.

ALL JOB POSTINGS ARE FREE



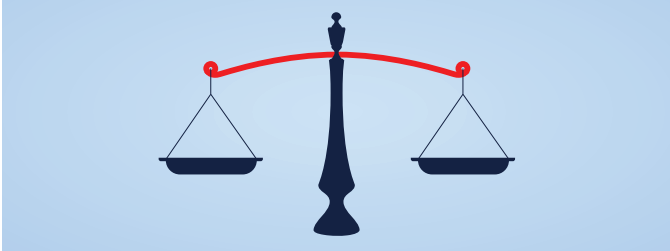
NJSBA members can apply for open positions for FREE.



Job openings will be advertised to the NJSBA's 18,000+ membership. All listings are for 30 days.

Visit
njsba.com
to find or
post a job

PRACTICE TIPS



ETHICS AND PROFESSIONAL RESPONSIBILITY

What is the Disciplinary Review Board and How Does its Decisions Affect the Level of Discipline Imposed on Lawyers?

By Bonnie Frost
Einhorn Barbarito

The Disciplinary Review Board (DRB) is an intermediate appellate tribunal appointed by the New Jersey Supreme Court and is made up of five lawyers, three lay persons and one retired judge [Rule 1:20-15(a)]. It reviews, *de novo*, ethics decisions rendered by local ethics committees and special masters which take testimony and receive evidence as to the grievance against an attorney. If there is a recommendation for discipline at the close of the hearing, then the DRB may hear oral argument or a respondent may agree to rely on the record without argument [Rule 1:20-15(f)].

After argument, the Board drafts a decision reached after discussion among the members and submits the underlying record including the ethics complaint, evidence submitted at the hearing, transcripts of any hearing, the ethics committee or special master's decision, and its decision, including any dissent, to the Supreme Court for the entry of an order which imposes discipline.

The Disciplinary Review Board determines the level of discipline which should be imposed upon a lawyer. However, it is only the Supreme Court which can enter an order for discipline order. Thus, the final determination of the level of discipline is solely within the purview of the Supreme Court. A decision of the DRB will become final once the Court enters an order, unless the respondent, the Office of Attorney Ethics or the Court on its own motion requests a review of the DRB's determination [Rule 1:20-16(b)]. The Supreme Court reviews the record *de novo*.

It is true that the Supreme Court adopts the DRB's recommendations approximately 90% of the time, and thus, the DRB's opin-

ion, more often than not, becomes binding and precedential.

The diversity of the backgrounds and experiences of the members of the Board, however, is integral to the decision-making process. It serves to ensure that the final decision is looked at from a variety of perspectives, not just one person's view of the facts.

The Supreme Court relies on the decisions of the DRB and takes note when a member or members of the Board write a dissent just as they take note when a decision is unanimous.

A dissent signals to the Court that the facts present an issue the DRB would like the Court to review. Take for example, the case of *In re Torre*, 223 N.J. 538 (2015). In that case, Torre "borrowed" \$89,250 from an unsophisticated 89-year-old client, a sum which comprised more than 70% of her estate. It appeared he had little intent of repaying the loan as he had made only two payments within a year of "borrowing" the money and in the 4½ years it took for the matter to arrive at the Supreme Court, he had made no payments to her or her estate as she had passed on shortly after his last payment in June 2009.

He never told the client to seek independent counsel even though he knew she relied upon him as she had designated him the executor of her will and had granted him a power of attorney. Even more disturbing to the Court was the respondent's attitude when he appeared before it. He showed no remorse as to his actions. The dissent prompted the Court to issue a written decision where Mr. Torre received a one-year suspension. This decision alerted lawyers of the Court's disapproval of lawyers who take advantage of elderly clients for their own benefit. This case established the precedent that such behavior will result in a one-year suspension, a level of discipline which was in excess of what the DRB has decided and even what the dissent had recommended.

Another example of the importance of the composition of the Board and how it can affect a disciplinary result is found in the case, *In the Matter of Jack N. Frost*, 171 N.J. 308 (2002). In that case, Frost obtained a loan from a client's settlement funds without appropriate safeguards for the client or a third party lienor after misrepresenting his finances, the true ownership of his assets, and his financial position to induce his client to participate in the loan. The Court noted that the dissent of two lay members was persuasive in making its decision to disbar him.

If a respondent faces disbarment as a result of a recommendation of disbarment from the DRB, or, if it believes the facts of a case and the record below requires the lawyer to defend themselves even if the ethical breach would not end in disbarment, it will issue an Order to Show Cause for the attorney to appear

before the Court and explain themselves as to “why they should not be disbarred or otherwise disciplined.”

Needless to say, one should show up if the Supreme Court asks for one’s presence. If one does not appear, invariably that respondent will be disbarred.

Even if one is facing a recommendation of disbarment, showing up and explaining oneself, can militate against harsh punishment. In the recent case of *Karina Pia Lucid*, 248 N.J. 514 (2021), a respondent who faced disbarment for knowing misappropriation of a client’s funds, was only censured. She showed up. She was contrite, did not use the funds for her own benefit and presented a sympathetic explanation that swayed the Court.

Next issue: Other Duties the DRB Performs for the Ethics System.



WORKING WELL

Don’t Just Practice Law— Practice Gratitude!

By Lori Ann Buza

NJSBA Lawyer Well-Being Committee Chair
KS Branigan Law

Gratitude breeds happiness. “It is not joy that makes us grateful, it is gratitude that makes us joyful,” theologian David Steindl-Rast once said. Instead of searching outward for others and/or things to find happiness...start with internalizing an appreciation for that which you already possess. Developing skills to *practice gratitude* will naturally foster a richer and more fulfilling life as an attorney. Plus, you can lead others (friends, family and even clients) to their own place of gratitude and joy.

What is gratitude? The Oxford dictionary defines it as, “the quality of being thankful; readiness to show appreciation for and to return kindness.” This quality of thankfulness and appreciation can certainly be a natural responsive feeling; but, I also believe it can be one’s *choice* to be grateful. And as a choice, it flows that feeling gratitude is in our *control*. It is largely conditional on our *attitude* in how we receive information, see others, and choose to identify and

interpret that which is around us. With conditioning and practice, including meditation, reflection, and mindfulness—the joy of feeling gratitude is possible for even the most fierce attorney.

The *benefits* of practicing gratitude are priceless. Overall mental and physical health improve with a significant decrease in the body’s stress response. Accordingly, the risk of heart disease, anxiety, depression, gastrointestinal conditions, headaches, back pain and other stress disorders may all reduce, as well as the decreased tendency for alcohol and substance abuse.

Practice, how? Start by thinking about your own individual list of what to be grateful for—your unique gifts and talents, your meaningful legal work, education, special moments, the people you cherish, your health and abilities, etc. Write them down, then re-visit this list each day, adding to it as you recognize more and more for which to be thankful. Bring your consciousness to a place of appreciation for what you acknowledge on your list. Do so in a quiet space and allow the feeling of thankfulness to subsume your thoughts and energy as you review your writing. Soon this list will become a journal...and then with practice, several journals. Go back and read them frequently.

Meditate for 10–20 minutes each day; schedule and prioritize it for yourself as you would any other client appointment. You may meditate quietly seated or laying down, with or without gentle music, unguided or guided (there are several apps you can use). Research what types of meditation are best for you. And remember, that even if you do not have time for formal meditation, you may engage in *meditative acts* (i.e. walking your dog, playing an instrument) which can be mindful experiences with similar benefits to meditation.

Breathe! Be sure to take time to appreciate nature by going for “outside” breaks from work, breathing in the fresh air, and visiting parks when time permits to observe the beauty and relish the oxygen-rich greenery. In all these moments, focus on your breathing and feel deep gratitude for the *breath* that sustains you. There are many breathing techniques you can learn that may help in your gratitude practice. Throughout your day, acknowledge and appreciate *all five of your senses* and what they explore and enjoy, with mindful reflection.

Make a point to express your thankfulness to *others* with smiles, compliments, and praise. Try to engage in volunteer and service work where the satisfaction of doing good can help *fill your gratitude cup*. Consistently, remind yourself throughout your day to have an optimistic perspective, and remember that it is largely *your choice* as to how you interpret your life’s unique fact pattern.

Buza’s ABCDs to practice gratitude:

Appreciate and acknowledge the good in your life.

Bring a positive attitude in how you see the world.

Control your thoughts and choose to be grateful.

Deliver kindness and the best version of yourself to others. ■



Our Best Programs. Viewable Wherever You Are.

Choose from
CLE On-Demand Videos
in every area of law.

- Featuring top experts.
- Earn CLE from any location.
- No complicated technology.

Order, Watch, and Earn Credits Immediately

Order and watch our on-demand video programs - 24/7 - from the convenience of your home or office! Anywhere your laptop, desktop, iPod, iPad, tablet or smartphone goes, you can be earning the credits you need.

Once you purchase your CLE On-Demand products, you'll receive an email with an access link and instructions to get started.
Note: You have 120 days from the date of purchase to view the program.

Here's how our On-Demand Video Seminars work:

- Select and purchase the program you would like to view
- View the program at your convenience (you have 120 days from the date of purchase)
- Your credits will be tracked automatically.

**Need CLE credits
fast? We've got
it covered.**

Earn 12 of your 24 New Jersey MCLE credits where and when it works for you: at home, on your commute, at the park, at the gym... anywhere your iPad, tablet or smartphone goes. You choose the method that works best for you.

CLE On-Demand programs are available in these areas of law:

- | | | |
|--------------------------------------|--------------------------------|----------------------------|
| - Animal Law | - Election Law | - Land Use Law |
| - Banking Law | - Environmental Law | - Law Office Management |
| - Bankruptcy Law | - Estate Law | - Local Government Law |
| - Business and Commercial Litigation | - Ethics | - Municipal Court Practice |
| - Business Law | - Family Law | - Patent and Trademark Law |
| - Civil Trial Law | - Federal Practice & Procedure | - Real Estate |
| - Construction Law | - General Law | - Renewable Energy |
| - Criminal Law | - Health Law | - School Law |
| - Dispute Resolution | - Immigration Law | - Taxation Law |
| - Diversity | - Insurance Law | - Workers Compensation |
| - Elder and Disability Law | - Labor and Employment Law | |

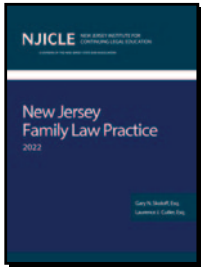
For a complete listing of programs, visit NJICLE.com

Available Now. Viewable Anywhere, Anytime from Any Device.

Visit NJICLE.com to place your order today.

**Voted New Jersey's
Top CLE Provider.**

NJICLE Publications



New Jersey Family Law Practice (2022, 16th Edition)

Packed with “how to’s” and helpful practice tips, this manual offers the foundation you need to advise your clients on divorce, annulment, custody, alimony, child support, equitable distribution, counsel fees, bankruptcy, taxation, domestic violence, stock options, and other related matters.

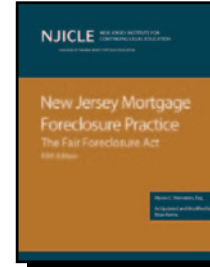
2-vol. Bound Book: \$299/\$239*



2022 Land Use Citator (2022, 15th Edition)

The Citator is a detailed and carefully ordered compendium of important cases, both reported and unreported, that allows you to read summaries of all significant cases and access them directly from your PC.

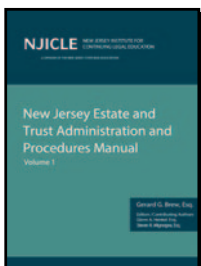
Treatise & CD w/hyperlinks: \$209/\$167*



New Jersey Mortgage Foreclosure Practice: The Fair Foreclosure Act (2021, 5th Edition)

This treatise provides a detailed background on foreclosure in general, plus a comprehensive analysis of the Fair Debt Collection Practices Act.

Bound Book & Forms CD: \$199/\$159*



NJ Estate and Trust Administration and Procedures Manual (2021)

This 2-volume set will help you navigate your way through the New Jersey estate administration maze. You'll get a CD-ROM for use as reference in your practice.

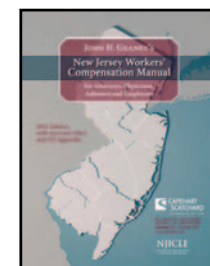
**2 Volume Bound Books and
Reference CD: \$325/\$260***



New Jersey Insurance Coverage Litigation - A Practitioners Guide (2021)

The book covers both first-party property and third-party liability coverage, and contains everything from a general overview of basic insurance principles to in-depth discussions of complex insurance and reinsurance issues.

Bound handbook: \$189/ \$151*



Geaney's New Jersey Workers Compensation Manual for Attorneys, Physicians, Adjusters, and Employers (2021)

The 2021 Manual is a compilation of prior editions with particular emphasis on cases decided in 2018-2020.

**Bound handbook and CD: \$249
(No other discounts apply)**

***NJSBA Member Price.**

Visit NJICLE.com to place your order today.

*



Treat Your Data Breach Investigation Like Your Toothbrush—Don't Share It with Anyone

By Daniel J. DeFiglio



DANIEL J. DEFIGLIO is a partner at Archer & Greiner, P.C. and a member of its business litigation, trade secret and noncompete, and cybersecurity practice groups.

No dentists have endorsed this statement. But several district courts—including ones within the Third Circuit—have (at least theoretically). Technology officers and corporate counsel should thus take heed: if you are not careful in responding to a data breach, your well-intentioned data breach investigation report could end up as “Exhibit 1” in later litigation.

This article will explore three recent federal court decisions related to the discoverability of so-called “data breach investigation reports,” and offer practical considerations based on those decisions.

Background

New Jersey requires “any business that conducts business in New Jersey” to disclose any “breach of security”—defined as “unauthorized access to electronic files, media or data containing personal information”¹—“in the most expedient time possible and without unreasonable delay.”² For purposes of this article, this is what is meant by a “data breach.”³

Following any data breach, businesses may undertake what is referred to as a data breach investigation. The scope and purpose for conducting a data breach investigation vary depending on the needs of the business. A larger company that handles an immense amount of financial or personal information, for example, may hire a specialized outside vendor to conduct a full-scale forensic examination of its computer environment. Smaller companies may investigate the matter internally (for example, with IT staff), or on a more-limited basis. For purposes of this article, a data breach investigation report refers to any written report that arises out of these investigations.

For many years, the discoverability—e.g., the ability of an adversary to obtain something through discovery in litigation—of these data breach investigation reports was somewhat unsettled. Several cases within the past two years, however, have begun to cement the resolution of this issue. Those cases, discussed more fully below, are *Capital One*,⁴ *Clark Hill*,⁵ and, recently, *Rutter's*,⁶ and provide several considerations for businesses faced with data breaches.

The *Capital One* Decision (May 2020)

The oldest of these cases is *Capital One*, which was decided in May 2020. The factual predicate of *Capital One* is probably familiar to most because it was reported in various nationwide news outlets.⁷ As a recap, “in March 2019 a data breach occurred whereby an unauthorized person gained access to certain types of personal information relating to Capital One customers.”⁸ Relevant here is Capital One’s response to that data breach.

According to the District Court opinion, in 2015, Capital One executed a master services agreement (MSA) with a company called FireEye, Inc. d/b/a Mandiant.

This MSA was then extended through a series of purchase orders and statements of work (SOW) for several years. In 2019, Capital One paid Mandiant a retainer for a SOW that entitled Capital One to 285 hours of services. The 2019 SOW included services like “computer security incident response; digital forensics, log, and malware analysis;...incident remediation,” and, in the event of a breach, a “detailed final report.”⁹

After the breach was discovered on or about July 19, 2019, Capital One hired an outside law firm to provide legal advice. The law firm retained Mandiant to “provide services and advice concerning ‘computer security incident response; digital forensics, log, and malware analysis; and incident remediation;’” in other words, the same services Mandiant was already providing under the 2019 SOW. According to the law firm’s agreement with Mandiant, Mandiant was to be paid in accordance with the terms of the MSA and 2019 SOW, but was to work at the direction of the outside law firm.

Following its investigation, Mandiant issued a report to the law firm detailing the technical factors that allowed the criminal hacker to penetrate Capital One’s security. The law firm provided a copy of the Mandiant Report to Capital One’s legal department, its board of directors, approximately 51 Capital One employees, four regulators (e.g. Federal Deposit Insurance Corporation, Federal Reserve Board, Consumer Financial Protection Bureau, and Office of the Comptroller of the Currency), and an outside accounting firm.

Despite acknowledging that litigation was foreseeable when Mandiant began its investigation (the first lawsuit was filed days after Capital One’s public announcement of the breach),¹⁰ the Court found that the Mandiant report was not privileged. In the Court’s view, the determinative issue was whether the

Mandiant Report “would have been prepared in substantially similar form but for the prospect of that litigation.”¹¹

The Court relied on at least three facts in finding the answer to this question was “yes” (meaning the report was not privileged). First, “Capital One had a long-standing relationship with Mandiant and had a pre-existing SOW with Mandiant to perform essentially the same services that were performed in preparing” the Mandiant Report.¹² Second, Mandiant was paid for its initial work under the Letter Agreement out of the retainer already provided to Mandiant under the 2019 SOW between Mandiant and Capital One.¹³ And third, Capital One’s disclosure of the Mandiant Report to outside regulators and an outside accounting firm—while not explicitly a waiver—was evidence that its investigation was “significant for regulatory and business reasons,” as opposed to in anticipation of litigation.¹⁴ Thus, the Court found that the Mandiant Report would have been prepared in a substantially similar form even if there were no prospect of litigation. Thus, it was not privileged.

The *Clark Hill* Decision (January 2021)

Clark Hill applied similar logic, but went a step further. In *Clark Hill*, the defendant claimed that it had conducted a “two-tracked investigation,” wherein its “usual cybersecurity vendor, called eSentry” investigated the data breach to preserve “business continuity;” a separate cybersecurity vendor (Duff & Phelps) conducted a second investigation for the “sole purpose of assisting [the outside law firm] in gathering information necessary to render timely legal advice.”¹⁵

While the Court did not appear to disagree with the two-tracked premise, it found that the defendant’s “two track story finds little support in the record,” meaning *Clark Hill* could not carry its

burden to show that the Duff & Phelps report was privileged. Of central importance to the Court's reasoning was: (1) there was "no evidence that eSentire ever produced any findings, let alone a comprehensive report like the one produced by Duff & Phelps;"¹⁶ (2) the Duff & Phelps report was "shared not just with outside and in-house counsel, but also with "select members of Clark Hill's leadership and IT team," and, later, the FBI;¹⁷ and (3) the defendant certified that it had used the report to manage "any issues . . . related to the cyber incident."¹⁸ Basically, the *Clark Hill* court found that although the defendant had "papered the arrangement using its attorneys," the

facts showed that Duff & Phelps' involvement (and, later, its report) had a much broader role than merely assisting outside counsel in preparation for litigation." Thus, the report was not privileged and had to be produced.¹⁹

The Rutter's Decision (July 2021)

*Rutter's*²⁰ reached the same conclusion, but for different reasons. There, Rutter's—a chain of gas stations and convenience stores—experienced a cybersecurity event on or about May 29, 2019. On the same day, Rutter's hired an outside law firm "to advise Rutter's on any potential notification obligations."²¹ The law firm then hired a third-party cybersecurity consultant—Kroll Cyber Security, LLC — "to conduct forensic analyses on Rutter's card environment and determine the character and scope of the incident."²² From there, Kroll gathered and analyzed "pertinent facts," including forensic images and "virtual machine snapshots of a sample of potentially affected in-store site controllers."

In total, Kroll's investigation took approximately two months, concluded in July 2019, and included a written data breach investigation report that later became the subject of a discovery dispute.²³ As in *Capital One* and *Clark Hill*, Rutter's asserted the report was protected by both the work product and attorney-client privileges. In determining that neither privilege applied, however, the Court relied on two key facts. First, the Court observed that Kroll's SOW "demonstrates that Defendant did not have a unilateral belief that litigation would result at the time it requested the Kroll Report."²⁴ Indeed, according to the Court, "[w]ithout knowing whether or not a data breach had occurred, Defendant cannot be said to have unilaterally believed that litigation *would* result."²⁵ Second, Rutter's corporate designee apparently testified that "Kroll would

have prepared—done this work and prepared its incident response investigation regardless of whether or not lawsuits were filed six months later[.]"²⁶

Practical Considerations

While every company will have different challenges and concerns in the event of a data breach, the above cases illustrate several considerations for C-suite level management and corporate counsel when conducting data breach investigations. Thematically, though, the primary consideration should be differentiation, *e.g.* how will the company show that the data breach investigation it seeks to protect was "different" than what it would have otherwise done.

Extrapolating from these cases, some factors to consider are:

1. Retaining outside counsel and experts specifically for the investigation you wish to shield; while this is not a determinative factor, *see, e.g., Capital One*, it can aid in this process of differentiation.
2. Clarifying the purpose of any SOWs to address specific legal issues that may arise in litigation, as opposed to merely assessing compliance with laws and regulations. This was a primary issue in *Capital One* and *Rutter's* and underscores the value of close collaboration between outside law firms and cybersecurity vendors in the early stages of a data breach response;
3. Using and describing techniques used in the investigation in the statement of work, and making sure that they are not the same as those used in assessing compliance with federal and state laws. As noted, that the 2019 SOW and Letter Agreement in *Capital One* described nearly identical services was an important consideration in the Court's ruling;
4. Treating each step of the investigation

TRADEMARK

& COPYRIGHT SERVICES

Trademark –
Supply word and/or design plus goods and services.

Search Fees:

- Combined Search - \$345
(U.S., State, Expanded Common Law and Internet)
- Trademark Office - \$185
- State Trademark - \$185
- Expanded Common Law - \$185
- Designs - \$240 per International class
- Copyright - \$195
- Patent Search - \$580 (minimum)

**INTERNATIONAL SEARCHING
DOCUMENT PREPARATION**

(for attorneys only – applications, Section 8 & 15,
Assignments and renewals.)

Research – (SEC – 10K's, ICC, FCC, COURT
RECORDS, CONGRESS.)

Approved – Our services meet standards set for us
by a D.C. Court of Appeals Committee

*Over 100 years total staff experience –
not connected with the Federal Government*

Government Liaison Services, Inc.
200 North Glebe Rd., Suite 321
Arlington, VA 22203
Phone: (703) 524-8200
Fax: (703) 525-8451
Major Credit Cards Accepted

Toll Free: 1-800-642-6564
WWW.TRADEMARKINFO.COM
Since 1957

as if it is work product from the beginning, and not merely “papering the file” as the Court observed in *Clark Hill*; and, finally

5. Not sharing the report outside the litigation control group. This was a factor in all three cases (hence, the title), wherein the breach investigation report was shared with, among others, outside regulators,²⁷ members of the company’s IT team,²⁸ and the FBI.

The above list is by no means exhaustive; there are certainly other things businesses could do that are not mentioned. Nor does following these steps ensure that a data breach investigation report will not be discoverable. Nevertheless, the lessons of these cases provide valuable insights that businesses may want to consider to protect their investigative reports.

Conclusion

Data breach investigations are valuable tools for businesses that have experienced a data breach. They can provide valuable insights to help better protect customer privacy, and can assist in responding to governmental authorities and private litigants. Yet the cases discussed herein highlight that these same advantages may also be a reason why well-intentioned reports may later become “Exhibit-1” at trial; namely, that the report was made to serve business purposes, not as a defense to litigation. Businesses must therefore be mindful of how these reports are created and shared so that they can obtain the full panoply of their benefits. ■

Endnotes

1. N.J.S.A. 56:8-161.
2. N.J.S.A. 56:8-163.
3. Because there is currently no federal data breach law, states are free to,

and have, adopted a patchwork of statutes that define the term differently. This article will not endeavor to explain the differences among the states.

4. For example, *Capital One*. See *In re Cap. One Consumer Data Sec. Breach Litig.*, No. 1:19MD2915 (AJT/JFA), 2020 WL 2731238, at *1 (E.D. Va. May 26, 2020), *aff’d*, 2020 WL 3470261 (E.D. Va. June 25, 2020).
5. *Guo Wengui v. Clark Hill, PLC*, 338 F.R.D. 7, 12 (D.D.C. 2021).
6. *In re Rutter’s Data Sec. Breach Litig.*, No. 1:20-CV-382, 2021 WL 3733137, at *1 (M.D. Pa. July 22, 2021).
7. [nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html](https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html)
8. *In re Cap. One*, No. 1:19MD2915 (AJT/JFA), 2020 WL 2731238, at *1.
9. *Id.*
10. *Id.* at *4 (“There is no question that at the time Mandiant began its “incident response services” in July 2019, there was a very real potential that Capital One would be facing substantial claims following its announcement of the data breach”)
11. *Id.*
12. *Id.*
13. *Id.* at *2.
14. *Id.* at *4.
15. *Clark Hill, PLC*, 338 F.R.D. at 11.
16. *Id.*
17. *Id.* at 12.
18. *Id.*
19. The court also found that the report was not privileged as an attorney-client communication the Duff & Phelps report (which it reviewed) was used to gain Duff & Phelps’s expertise in cybersecurity, not in obtaining legal advice from its lawyer. *Id.* at 13.
20. *In re Rutter’s*, No. 1:20-CV-382, 2021 WL 3733137, at *1.
21. *Id.*

22. *Id.*
23. *Id.*
24. *Id.* at *2. Kroll’s SOW apparently described its services as an investigation “to determine whether unauthorized activity within the Rutter’s systems environment resulted in the compromise of sensitive data, and to determine the scope of such a compromise if it occurred.” *Id.*
25. *Id.*
26. *Id.* Applying reasoning similar to *Clark Hill*, the Court also found that Kroll’s report was not subject to the attorney-client privilege because it discussed “facts,” not “opinions” or “tactics.” *Id.* at *3.
27. *In re Cap. One*, No. 1:19MD2915 (AJT/JFA), 2020 WL 2731238, at *2.
28. *Clark Hill, PLC*, 338 F.R.D. at 12 (“select members of Clark Hill’s leadership and IT team”); see also *In re Rutter’s*, No. 1:20-CV-382, 2021 WL 3733137, at *3 (explaining the report was shared with Rutter’s IT personnel).



Defining Privacy of Biometric Information

Legislative Approaches to Growing Use
of Biometrics in Our Society and What
it Means for Businesses

By Brett R. Harris and Natalie Moszczynski

The use of biometric identifiers is not a new concept. The sci-fi and action-thriller media of the late 20th century touted retinal scans as a means to access bank vaults and facial recognition to track the location of villains as spy gadgets, which didn't truly exist in day-to-day life. Nowadays, these concepts are no longer futuristic and unrealistic, and instead are entirely believable and in use. Biometric information use ranges from medical practices to security and police agencies, from employment agencies to social media companies, and is even collected at amusement parks.

Following this uptick in biometric data collection, there also has been an increase in biometric data privacy laws both enacted and proposed, along with an increase in legislation to ensure adherence and protect consumers. Currently a dichotomy exists where some states have created their own tailored legislative mechanisms to protect consumers specifically with respect to biometric information, whereas other states incorporate biometric information as part of their definitions of what consumers are protected from in already existing privacy laws. Since New Jersey clients may be affected by this patchwork of nationwide laws, this article addresses this issue and sets forth an overview of the intersection of privacy and biometric data laws.

What is Biometric Information

The legal definition of biometric information or identifiers varies by state. As of now, no overarching federal regulation of biometric information exists. The only federal privacy mechanism that the government may apply is Section 5 of the Federal Trade Commission Act which applies to unfair or deceptive acts or practices in commerce.¹

States have taken it upon themselves to pass legislation defining biometric data, whether including it as a lone definition or expanding existing definitions of personal information to include biometric identifiers. Biometric information can be generally described as metrics of physical personal characteristics that belong to each individual such as, but not limited to, the sound of one's voice, a fingerprint, or a photo of a face or retina. A sample of how biometric information and biometric identifiers are defined in the first biometric legislation, Illinois' Biometric Information Privacy Act (BIPA), is as follows:

'Biometric Identifier' means a retina or iris scan, fingerprint, voice-print, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening,

demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.... 'Biometric Information' means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.²

Each state appears to define biometric data differently. While BIPA has a very extensive definition of biometric information in its legislation, states that have included biometric information in existing laws have a tendency to more generally explain biometrics. This is not always the case, but is more likely when no current biometric specific legislation is in place. For example:

Vermont

As part of its consumer protection privacy laws, Vermont refers to biometric information within the definition of "brokered personal information," which is a computerized data element about a consumer meant for the dissemination to third parties. Biometric data falls under a subset of brokered personal information defined as "unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data."³



BRETT R. HARRIS, is a shareholder on the Business Law team at Wilentz, Goldman & Spitzer, P.A. Known as a Business, Nonprofit and Technology Attorney, she is admitted in New Jersey and New York with a broad-based general corporate practice consisting of both transactional matters and client counseling on everyday business matters with a focus on technology and IP issues. She also has a particular focus of representing nonprofit organizations, foundations and tax-exempt entities.



NATALIE MOSZCZYNSKI is an associate on the Business Law Team with Wilentz, Goldman & Spitzer, P.A., where she focuses her legal practice in health law, corporate law and cannabis law.

California

California is the most inclusive. It deems biometric information to be a varietal of personal information.⁴ However, the California legislature took the additional step of stating that while personal information is typically information that is not publicly available, biometric information is an exception, and it cannot be derived off of publicly available information even if such public access exists. The definition of biometric information in the California Consumer Privacy Act is as follows:

...an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health or exercise data that contain identifying information.⁵

Virginia

The Virginia Consumer Data Privacy Act (VCDPA) will come into effect on January 1, 2023, and defines biometric data as “data generated by automatic measurements of an individual’s biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. ‘Biometric data’ does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.”⁶

Due to the prevalence with which

such information is being obtained and stored, states have been passing legislation toward protecting their consumers by providing them with privacy rights over whether such information can be stored at all, what information may be collected, whether it may be provided to outside third parties, and what a company must do in the case of a security breach. The main difference between biometrics and certain other personal data currently protected in consumer privacy laws is that biometric information is specific to each person. For instance, while a password can be changed routinely and periodically, an individual’s retina is much less likely to be altered. Biometric information is extremely individualized and thus can provide heightened security. But, it obviously comes with a heightened risk of vulnerability.

Current State of Biometric Information in Legislation

Only a few states have enacted legislation specific to biometric data collection, the consents required to collect such information, and penalties applicable if the laws are disregarded. These states include Illinois, Texas, and Washington. As mentioned earlier, some states have simply chosen to include biometric data restrictions into existing consumer privacy legislation, such as California, Virginia, Vermont, Maryland, Arkansas and Colorado. The benefit of having a biometric specific law is that it allows states to specify interaction with such data – especially since it is not always exclusively collected for security purposes. The biometric privacy laws institute regimes that require consent and notice be provided to consumers in a more stringent manner than those in existing consumer privacy legislation. States that have adopted biometric information as part of their definitions for personal identifying information tend

to lack the specificity that biometric privacy laws maintain. For instance, Colorado states that “A covered entity that maintains, owns, or licenses personal identifying information (including biometric information) must develop a written policy for the destruction and disposal of all paper and electronic documents containing personal identifying information for the disposal of such information such as by shredding, erasing, or otherwise modifying the personal identifying information in the paper or electronic documents to be unreadable or indecipherable and must implement and maintain reasonable security procedures and practices.”⁷ Its consumer protection act does not require consent, nor does it require that the consumers potentially implicated must be notified of the written plan.

Biometric specific laws are being proposed throughout the country, including in states that have altered the definition of personal identifying information (also known as PII) in existing privacy legislation, because they recognize the sensitivity inherent to biometric identifiers and therefore provide greater restrictions for the security of the consumer. These restrictions tend to provide that consumers have a right to request disclosure of any and all personally identifying information, including biometric identifiers collected about the individual consumer, providing them with the ability to request deletion of such information, allowing them to opt out of provision of such information or its further sale to third parties, and giving consumers notice of the length of time for which such data will be maintained by a business.

Biometric Specific Legislation

Illinois was the first state to regulate how biometric data is used, collected, and disclosed by enacting BIPA in 2008.⁸ A major stand out between the Illinois

law and other state laws is that the main method of enforcement of BIPA is through private right of action.

BIPA requires any private entity that possesses biometric information or identifiers to develop and make publicly available a written policy that includes a retention schedule and guidelines for permanently destroying the biometric identifiers and biometric information when the initial purpose for collecting or obtaining it has been satisfied or within 3 years of the individual's last interaction with the entity, whichever occurs first. Furthermore, a private entity may not collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or information unless it first provides the individual with (1) a written statement that the data will be collected or stored and (2) detailing the specific purpose and retention period for the collected biometric data and (3) obtains a written release from the individual, and BIPA sets forth similar restrictions on a private entity's ability to disclose such information to outside parties.⁹ It is important to note that BIPA grants aggrieved individuals a private right of action to sue for a mere violation of the law's requirements even if the individual does not suffer actual injury.¹⁰

Alongside BIPA, Texas has enacted the Texas Statute on the Capture or Use of Biometric Identifier[s]¹¹ and Washington passed H.B. 1493 in 2017,¹² as the second and third states to enact such legislation, respectfully. The similarities among the three legislations are quite distinct. Biometric data may not be stored longer than is necessary after its initial purpose has been completed. Consent is another highly important condition, and although the process in which consent and notice are given vary by state, the fact that a consumer must agree to their biometric information being collected is

an unchanging standard. The bills have several differences. The most noticeable is that BIPA offers private citizens a right to bring suit against companies that do not properly follow the provisions, whereas Texas and Washington have not included such language in their legislation, instead allowing only government actors to bring suit against companies.

New Jersey Proposals for Biometric Privacy Laws

So how do these laws affect New Jersey? The implementation of these regulations throughout certain states, along with the consistent proposals for similar New Jersey legislation, requires businesses to plan ahead to shield themselves from liability, whether it be from consumers across the country or even those in New Jersey. Over the past few years, New Jersey has proposed legislation to regulate collection, usage, and storage of biometric data.

One of the features of the most recently proposed New Jersey legislation has been that whenever biometric data is to be used, a written consent must be obtained from the individual providing data.¹³ The New Jersey proposal follows similar requirements to those imposed by BIPA; however New Jersey has included that the written release provided by the individual must also be executed¹⁴—a feat that may not always be possible, especially in the context of who collects biometric data. For instance, biometric data often is collected through a smartphone via a fingerprint or facial recognition software or by a website. While it is in essence possible for that entity to send consent to be electronically signed by their consumer, it may make data collection an onerous process. Drawing out the process that people are currently used to, such as checking a box to agree to the terms and conditions of a website, may lessen a consumer's desire to read the

terms to which they are consenting. But more difficult is the potential of biometric information being collected from the general public when, for example, they enter a store using biometric data collection as a form of security. It is highly unlikely that every passerby would execute a formal consent in such a scenario, making it difficult to implement use of such biometric data as a security method. Legislation could facilitate such usage by lowering the means of consent, such as by simplifying the standard to informed consent or reasonable notification so that any potential individual whose biometric information is being collected is aware of such. At the commencement of New Jersey's 220th Legislative Session in early 2022, proposed legislation regarding biometrics had yet to be sponsored.

Concerns For Businesses

Businesses have different concerns depending upon their intended use of biometric data. Many businesses have collected biometric information across state lines via the internet. Because of the expansiveness of today's internet age, should private actors abide by the strictest applications of BIPA to shield themselves from potential litigation risk? And how would they take steps to protect themselves from such liability? The first step a business should take is to investigate the extent of their insurance coverage to ascertain if it applies in the case of a security breach involving biometric information. Cybersecurity policies do not always assume the collection and maintenance of biometric information and the business should conduct a risk assessment with knowledge of any limits of coverage. Additionally, many states, albeit not all, extend their biometric privacy and consumer privacy legislations to all consumers, irrespective of where their biometric data is being processed,

collected, or maintained; therefore, if a business were to use the biometric information of an Illinois resident, they would find themselves subject to BIPA even without any presence of the business in Illinois.

Businesses have the option to act in the most conservative manner and abide entirely by the requirements of BIPA for private entities who are involved in processing biometric information. This would require stringent compliance, because “no private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person’s or a customer’s biometric identifier or biometric information unless: 1) the subject of the biometric identifier or biometric information or the subject’s legally authorized representative consents to

the disclosure or redisclosure; 2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject’s legally authorized representative; 3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or 4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.”¹⁵

Providing notice regarding the collection and maintenance of such information, ensuring reasonable security and maintenance of such information, and requiring consent from consumers are positive initial steps to take to encourage legal compliance as more states consider passing legislation regarding biometric information. ■

Endnotes

1. 15 U.S.C.A. § 45 (5).
2. 740 Ill. Comp. Stat. Ann. 14/10.
3. Vt. Stat. Ann. tit. 9, § 2430 (1)(A)(vi).
4. Cal. Civ. Code § 1798.140 (o)(1)(E).
5. Cal. Civ. Code § 1798.140 (b).
6. Va. Code Ann. § 59.1-571.
7. Colo. Rev. Stat. Ann. § 6-1-713; *See also* Colo. Rev. Stat. Ann. § 6-1-713.5.
8. 740 Ill. Comp. Stat. Ann. 14.
9. *Id.* at 14/15.
10. *Id.* at 14/20.
11. Tex. Bus. & Com. Code Ann. § 503.001.
12. Wash. Rev. Code Ann. § 40.26.
13. 2020 New Jersey Assembly Bill No. 3625, New Jersey 219th Legislature - Second Annual Session.
14. *Id.* at Section 4(b).
15. 740 Ill. Comp. Stat. Ann. 14/15.




demand integrity ✚

character matters in the courtroom as justice is never blind to seeking truth. Withum and our team of top forensic and valuation professionals know what it takes to build a winning case. Attorneys of defendants and plaintiffs alike value our unwavering integrity and success record of trying and settling hundreds of cases.


Visit us online to learn more about our Forensic and Valuation Services.

withum.com



The New Jersey State Bar Association Insurance Program

Advised and
administered by



We put doctors &
lawyers
together.

USI Affinity is endorsed by the New Jersey State Bar Association for our expertise in designing affordable Health Insurance solutions for law firms.

Changes in health care law may impact you, your firm or your family. Finding affordable, quality coverage is now more important than ever — and that's where we come in.

The benefits specialists at USI Affinity are experts in Health Care Reform. We can help you design a health plan that provides the best coverage and value while ensuring you will be in compliance with complex new regulations and requirements.

Introducing the NEW NJSBA Insurance Exchange, an online marketplace to help you find the coverage you need.

We've made it simple to browse through options online and find individual or group benefit plans, no matter what the size of your firm or practice. Log on now to find coverage for:

- **Medical**
- **Dental**
- **Vision**

Visit the NJSBA Exchange at www.usiaffinityex.com/njsba to find affordable coverage options for you, your family and your practice.

Need guidance? Call 855-874-0267 to speak with the experts at USI Affinity, the New Jersey State Bar Association's endorsed broker and partner for 60 years.



What Every In-House Attorney Should Know About Preserving the Confidentiality of Forensic Reports Related to a Security Incident

By Angelo A. Stio III, Avrohom C. Einhorn, and Brianna M. Alunni

Businesses involved in a cybersecurity incident face unique challenges when it comes to conducting a prompt investigation while still protecting the process and results of that investigation from disclosure under the attorney-client privilege and work product doctrine. This article highlights a number of federal court decisions that discuss the pitfalls encountered with engaging a forensic consultant to perform an investigation of a security incident and provides guidance on ways to enhance the chances of preserving the confidentiality of a forensic report and communications related thereto,¹ including any draft reports.

Federal Court Cases

Federal court decisions addressing the disclosure of forensic expert reports related to security incidents demonstrate that disclosure or non-disclosure turns on facts specific to the particular incident in question. With this principle in mind, we selected five decisions to highlight instances when a court ordered disclosure of a forensic report or determined that the report and/or communications related thereto were protected from disclosure.

In re Target Corp. Customer Data Security Breach Litigation

In *In re Target Corp. Customer Data Security Breach Litigation*,² the Court reviewed a motion to compel production of documents and communications relating to a Data Breach Task Force's response to a security incident. Target responded to the incident by undertaking a two-track investigation involving (1) an "ordinary-course investigation," which it described as one set up so that it could learn how the breach occurred and respond to it appropriately; and (2) a Data Breach Task Force inquiry, which was conducted, to "provide Target with legal advice" in anticipation of litigation. During discovery, Target disclosed the material related to its ordinary-course investigation but refused to produce the Task Force's materials on the basis that they were covered by the attorney-client privilege and/or work product doctrine.

The plaintiffs filed a motion to compel claiming the materials were subject to disclosure because they would have been prepared regardless of any litigation. The plaintiffs noted that "Target would have had to investigate and fix the data breach regardless of any litigation in order to appease its customers, ensure continued sales, discover its vulnerabilities, and protect itself against future breaches."

After an in camera review, the Court held that documents and communications relating to the work of the Task Force were protected because the Task Force's work "was focused not on remediation of the breach, as Plaintiffs contend, but on informing Target's in-house and outside counsel about the breach so that Target's attorneys could provide the company with legal advice and prepare to defend the company in litigation that was already pending and was reasonably expected to follow." The Court, however, granted the motion to compel as to communications with Target's Board of Directors concerning "Target's business-related interests...in response to the breach" because it held that those communications were neither made for the purpose of obtaining legal advice nor in anticipation of litigation.

Accordingly, *Target* reveals that if a separate track for an investigation occurs for the purpose of providing legal advice in anticipation of litigation, the chances of preserving confidentiality are increased.

In re Experian Data Breach Litigation

In *In re Experian Data Breach Litigation*,³ the Court addressed whether plaintiffs could compel production of a forensic report and related documents prepared by a third-party forensic expert following a security incident. Experian insisted that the report was protected by the attorney-client privilege and work product doctrine while the plaintiffs argued that it was not protected because it was not prepared for the purpose of litigation. Applying the "because of" test articulated by the Ninth Circuit in *In re Grand Jury Subpoena (Mark Torf/Torf Envtl. Mgmt.)*,⁴ the Court held that the report was protected from disclosure under the attorney work product doctrine. Under this "because of" test, if a "document was created because of anticipated liti-



ANGELO A. STIO III is a partner at Troutman Pepper Hamilton Sanders LLP and a member of the firm's Cybersecurity, Information Governance, and Privacy Group. He practices out of the firm's Princeton office.



AVROHOM C. EINHORN is an associate at Troutman Pepper Hamilton Sanders LLP and a member of the firm's Cybersecurity, Information Governance, and Privacy Group.



BRIANNA M. ALUNNI is an associate at Troutman Pepper Hamilton Sanders LLP and a member of the firm's Health Sciences Department.

gation, and would not have been created in substantially similar form but for the prospect of that litigation,” it constitutes attorney work product and is not subject to disclosure.

The *Experian* Court found the report to have been prepared in anticipation of litigation, “even if that wasn’t [the expert’s] only purpose.” This finding was based on the determination that “but for the anticipated litigation, th[is] report wouldn’t have been prepared in substantially the same form or with the same content.” The Court’s rationale was grounded primarily in the report not being given to Experian’s Incident Response Team or other personnel working on remediation of the systems and instead being limited to only being shared with the legal team. The Court held that “[i]f the report was more relevant to Experian’s internal investigation or remediation efforts, as opposed to being relevant to defense of this litigation, then the full report would have been given to th[e] [non-legal] team.”

In re Dominion Dental Services USA Inc. Data Breach Litigation

In *In re Dominion Dental Services USA Inc. Data Breach Litigation*,⁵ the Court decided that a forensic report, prepared by a cybersecurity firm hired to investigate and remediate a data breach of Dominion’s systems was not protected by the work-product doctrine. The Court’s holding was grounded in its determination that the report was prepared for the prevention of and response to a data breach, rather than for litigation.

The Court applied the “driving force” test used by the Fourth Circuit where there are dual motives behind the preparation of a particular document, such as both litigation and business purposes.⁶ The Court determined that the “driving force” behind the agreement between Dominion and the report’s writers was

not litigation, but rather, incident response support and business purposes. In making this determination, the Court rejected (a) an affidavit from a Dominion employee asserting that the report would not have been prepared without the threat of litigation and (b) the language from the Statement of Work (SOW) referencing “under the direction of Counsel” as bare assertions made for the sole purpose of protecting the report. The Court’s finding was grounded in (1) the report stemming from an agreement substantially similar to one entered into between the parties *before* the breach and articulating the same deliverables, including written response reports and (2) Dominion publicizing the forensic expert’s work for non-litigation purposes, “such as reassuring customers and communications strategy.”

Importantly, the Court left open the possibility that draft reports or other related communications would still be protected by attorney-client privilege or the work product doctrine.

In re Premera Blue Cross Customer Data Security Breach Litigation

In *Premera Blue Cross Customer Data Security Breach Litigation*,⁷ the Court addressed a motion to compel various documents, including a third-party vendor’s work on a security incident investigation and remediation for Premera. Premera refused to disclose documents related to the third-party vendor’s work on the basis that it was protected by the attorney-client privilege and work-product doctrine. Premera argued that these documents were prepared primarily for the purpose of litigation and for the purpose of facilitating legal advice. The Court disagreed and found that these documents were not protected by either doctrine.

In making its finding, the *Premera* Court first evaluated whether documents

drafted in response to the realization of a security incident, including press releases and customer notices, were privileged under the standard set by the Washington Supreme Court in *Morgan v. City of Fed. Way*.⁸ In *Morgan*, the Washington Supreme Court held: “a document prepared for a purpose other than *or in addition to* obtaining legal advice” is not privileged. The *Premera* Court found “[t]he fact that Premera planned eventually to have an attorney review those documents or that an attorney may have provided initial guidance...does not make every initial draft and every internal communication” privileged. Next, the *Premera* Court found that documents prepared by third-party vendors, even those retained by Premera’s outside counsel, were not privileged simply because they were “delegated to [Premera’s] outside counsel for supervision,” if they were in-fact intended to perform a business function. The *Premera* Court also found that these documents were not protected by the work-product doctrine because under the 9th Circuit’s “because of” test,⁹ Premera failed to demonstrate these “documents were created because of litigation rather than for business reasons” or that the documents would have been prepared any differently if litigation was anticipated.

The *Premera* Court reached similar conclusions with regard to the disclosure of a remediation report prepared by a third-party cybersecurity firm that was hired by Premera before it discovered malware and before it retained outside counsel. While Premera and the cybersecurity firm amended the language in the SOW after Premera retained outside counsel to direct outside counsel as the supervisor, the Court found this lone update insufficient to render the reports privileged. Like *Experian*, however, the Court left open the possibility that communications “sent to or from counsel

seeking or providing actual legal advice, such as about possible legal consequences of proposed text or an action being contemplated by Premera,” would be privileged.

Guo Wengui v. Clark Hill, PLC

More recently, in *Guo Wengui v. Clark Hill, PLC*,¹⁰ the Court addressed whether the defendant, Clark Hill, was required to produce a copy of a third-party forensic investigation report prepared following a security incident. The Court ruled that the forensic report was not covered by the attorney-client privilege or work product doctrine and required the report’s disclosure.

The *Guo Wengui* Court applied the D.C. Circuit’s “because of” test, which is similar to the Ninth Circuit’s test and asks “whether, in light of the nature of the document and the factual situation in the particular case, the document can fairly be said to have been prepared or obtained because of the prospect of litigation,” to determine that the report was not covered by the work product doctrine. The Court found that the report was a necessary business function that would have been created regardless of litigation based on the report’s dissemination to the defendant’s non-legal team, including its leadership and IT personnel, and to the FBI. Under these circumstances, the Court found the report was not covered by attorney-client privilege or work product doctrine because the purpose of the report was to obtain the expert’s cybersecurity expertise and not to facilitate legal advice being provided to the client.

Key Takeaways

These decisions demonstrate the fact-sensitive inquiry courts will conduct to determine whether a forensic investigation report and related communications are discoverable. While there is no guar-

antee that a forensic investigation report, draft reports and related communications will remain confidential, the decisions provide guidance on the following steps that can be employed to improve the chances of successfully asserting attorney work product and attorney-client privilege protections in response to a request to disclose:

If a business suspects a security incident, outside counsel should be involved at the outset, especially before any forensic consultant is engaged and any investigation is performed.

- **Retention of Outside Counsel.** If a business suspects a security incident, outside counsel should be involved at the outset, especially before any forensic consultant is engaged and any investigation is performed. The retention of counsel at the outset will enable a business (and counsel) to develop a strategy for communications and the investigation that considers the attorney-client privilege and attorney work product protections available for reports, draft reports and communications. As part of any strategy analysis, a business may want the forensic report to be disclosed to create a factual account

of what occurred so it could be shared with others, including regulators. Outside counsel is nevertheless important to help in making this determination and in implementing a strategy to protect the attorney-client privilege and/or work product protections that may be available with respect to draft reports or communications related to the investigation or incident response. Both the *Dominion* Court and the *Premera* Court left open the possibility that draft reports or related communications would be protected under attorney-client privilege.¹¹

- **Retention of a Forensic Investigator.** Any forensic investigator should be engaged by outside counsel and should perform work at the direction of outside counsel from the outset. Moreover, the forensic investigator’s work should be performed for the purpose of enabling counsel to provide legal advice to the client.
- **Ensure the language of the contract or SOW supports the invocation of attorney work product and attorney-client privilege protections.** The federal court decisions also reveal that the language of the forensic investigator’s contract or statement of work (SOW) will help determine the applicability of the attorney work product and attorney-client privilege to a forensic investigation report and related communications. The contract or SOW should make clear that the forensic consultant is being engaged by counsel for the purpose of enabling counsel to provide legal advice to the client. In addition, in light of the significant number of litigations being filed in response to security incidents, the contract or SOW should note that the forensic consultant’s work is in anticipation of litigation and claims that may be asserted.

- **Outside counsel should control communications.** Once retained, communications, including working through draft reports and other strategic decisions with the forensic consultant, should go through outside counsel. The chances of successfully preserving the confidentiality of a forensic report and related communications, including draft reports, will increase if counsel takes the lead on all meetings and communications with the forensic consultant. Stated differently, it will be difficult to contend that forensic work is being conducted under the direction of counsel, if the forensic consultant is not communicating directly with outside counsel. Further, communications with the forensic consultant should be limited to those people necessary to enable outside counsel to provide legal advice and should be designated with appropriate disclaimers identifying the communication as constituting attorney work product and being subject to the attorney-client privilege.
- **Limit dissemination of any forensic report.** One of the important factors the *Experian* Court relied on to find the forensic report was protected under the attorney work product doctrine, was the fact that the dissemination of the forensic report was limited to outside counsel and in-house counsel and not widely disseminated to the information security team and IT department. Similarly, one of the most important factors the *Guo Wengui* Court relied on to find that the forensic report was for a business purpose and not protected was the report's dissemination to the defendant's non-legal team, including its leadership and IT personnel, and to the FBI. Limiting dissemination also helps avoid the pitfall of a corporate designee testifying that the investiga-

tion report would have been prepared regardless of whether there was litigation pending. While limiting disclosure may mean that a business may need to prepare a separate report to determine such things as the personal information that was compromised, that separate report would be purely factual in nature and used solely for the purpose of providing notice and not providing legal advice.

Responding to a security incident is complex and requires a nimble and thoughtful approach by experienced professionals who can develop a strategy from the outset. As outlined above, federal courts will look at various factors to determine whether forensic investigation reports and related communications should be afforded work product and attorney-client privilege protections. The ability to demonstrate that the report and communications are anchored to legal advice and strategy and in anticipation of litigation, increases the chances of preserving confidentiality. In contrast, if the information in a report or communication is factual in nature, widely disseminated, and would have been prepared regardless of whether litigation was anticipated, the ability to preserve confidentiality is significantly decreased. Retaining counsel, following some simple steps, and having a strategy in place will increase the likelihood that privilege and work product protections are not waived and the forensic report and communications are not subject to disclosure. ■

Endnotes

1. "Communications" refer to communications between counsel and the forensic consultant. Communications regarding the report or strategy that take place

between counsel alone or between counsel and the client could be protected under attorney-client privilege or work product doctrine.

2. No. 14-cv-2522, 2015 WL 6777384 (D. Minn. Oct. 23, 2015).
3. No. 15-cv-01592 AG, 2017 WL 4325583 (C.D. Cal. May 18, 2017).
4. 357 F.3d 900, 907-08 (9th Cir. 2004).
5. 429 F. Supp. 3d 190 (E.D. Va. 2019).
6. *Nat'l Union Fire Ins. Co. of Pittsburgh, Pa. v. Murray Sheet Metal Co.*, 967 F.2d 980, 984 (4th Cir. 1992).
7. 296 F. Supp. 3d 1230 (D. Ore. 2017).
8. 213 P.3d 596 (Wash. 2009).
9. *See U.S. v. Richey*, 632 F.3d 559, 567 (9th Cir. 2011) (holding documents prepared for dual purposes "deemed prepared because of litigation if 'in light of the nature of the document and the factual situation in the particular case, the document can be fairly said to have been prepared or obtained because of the prospect of litigation.'").
10. 338 F.R.D. 7 (D.D.C. 2021).
11. *See also In re Premera Blue Cross Customer Data Security Breach Litigation*, 329 F.R.D. 656, 661 (D. Or. 2019) ("Draft documents prepared by attorneys, at the request of attorneys, or otherwise prepared by Premera employees or third-party vendors, and sent to and from attorneys for legal advice relating to those drafts, are likely subject to the attorney-client privilege or work-product protection").



REACH

Beyond

Power your law practice with industry-leading legal research. Fastcase is a free member benefit of the New Jersey State Bar Association.

 fastcase®

LEARN MORE AT WWW.TCMS.NJSBA.COM

DOWNLOAD TODAY





Retaining Privacy with Non-Waiver Orders

By Veronica J. Finkelstein

Consider this scenario: You represent the owner of a condominium complex suing its general contractor. The owner experienced problems during construction that delayed the completion of the project by more than a year. The delay had a ripple effect, causing each phase of construction to be more expensive than anticipated. What is worse, the delay caused nearly all the unit owners to rescind their contracts. Your client has lost millions of dollars.

The general contractor asserted cross claims against dozens of subcontractors and material suppliers. The case will be complex with voluminous discovery. Your client seeks to minimize discovery costs as much as possible, citing losses already experienced during construction.

The complex's in-house counsel was heavily involved in the project as it was ongoing. A cursory review of your client's documents reveals dozens of attorney-client privilege and work product protected documents scattered between discoverable contracts, subcontracts, and change orders.

Discovery will consume significant recourses. As a partner in a small firm, scrutinizing every page of your client's voluminous records seems infeasible. But if you do not, you are certain some of your client's private, privileged information will be disclosed. You are starting to question whether you should have accepted the case in the

first place. The problem seems insurmountable.

There is a solution—and it is a solution endorsed by the Sedona Conference, which recently issued commentary addressing this very issue. This article provides the highlights of that commentary.

The Sedona Conference is a nonprofit legal policy research and education organization comprised of judges, attorneys, and non-legal experts.¹ The Sedona Conference focuses on electronic discovery and routinely promulgates commentary and other guidance. Last year, the Sedona Conference circulated its “Commentary on the Effective Use of Federal Rule of Evidence 502(d) Orders,” which will be formally published this year.² Whether you practice in New Jersey state or federal courts, Rule 502(d) orders (known informally as “non-waiver orders”) are an important tool to help you safeguard your client’s privacy.

Federal Rule of Evidence 502(d) and New Jersey Rule of Evidence 530(c)(4)

Federal Rule of Evidence 502 was enacted in 2008 and is Congress’s effort to minimize the exorbitant cost of civil discovery without requiring that litigants risk broad waivers of privilege. Under Rule 502(d), a federal court may enter an order that “privilege or protection is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in any other federal or state proceeding.”³ In other words, if the parties so request, the presiding court can enter a non-waiver order at the outset of discovery as a fail-safe in the event a privileged document is produced. Even if attorney-client privilege or work product protected information is disclosed, such disclosure may not operate as a

waiver of all protected information.

The New Jersey Rules of Evidence were amended effective July 1, 2020, to track the language of Federal Rule 502(d). Under New Jersey Rule 530(c)(4), a New Jersey court may order that “privilege or protection is not waived by disclosure connected with the litigation pending before the court, in which event the disclosure is also not a waiver in any other federal or state proceeding.”⁴ New Jersey Rule 530 now contains the same safe harbor as Federal Rule 530(d). If a New Jersey court has entered a non-waiver order at the request of the parties, disclosure of privileged information does not waive the privilege.

Neither subsection of the rule is limited to inadvertent disclosure. Rather, these subsections are broader. A non-waiver order may apply to all disclosures, inadvertent or not.

The amendment to New Jersey Rule 530 tracking the language of Federal Rule 502 means that the extensive caselaw analyzing Federal Rule 502 is now instructive in interpreting New Jersey Rule 530. This means that although the amendments to New Jersey Rule 530 are recent, there is already a robust body of authority that may prove relevant in understanding the contours of New Jersey Rule 530.

The Primary Benefits of Non-Waiver Orders

The Sedona Conference favors non-waiver orders and encourages litigants to consider entering into them. Non-waiver orders have two primary benefits.

First, non-waiver orders provide predictability and uniformity. Without such an order, waiver occurs unless the party disclosing the information can demonstrate that the disclosure was inadvertent.⁵ This is a fact-sensitive inquiry, and it can impose a significant burden on the

party attempting to preserve privilege. In assessing whether disclosure was inadvertent, courts have considered various factors including: (1) the reasonableness of the precautions taken by the lawyer; (2) the passage of time between the disclosure and efforts to claw back the disclosed information; (3) the scope of the disclosure and (4) the interests of fairness. There is no way to determine in advance whether disclosure will be held to be inadvertent or not.

In contrast, with a non-waiver order in place the results are predictable and uniform—disclosure is not tantamount to waiver. If information has been disclosed, it can be clawed back without need to consider the circumstances surrounding the disclosure.

Second, non-waiver orders discourage judicial second-guessing of discovery methods. Without such an order, any attempt to claw back privileged information will require that party’s lawyer disclose the circumstances under which the information was disclosed. The presiding court will then rule on whether the pro-



VERONICA J. FINKELSTEIN is a 2004 graduate, with honors, of the Emory University School of Law and 2001 graduate, with dual honors, of the Pennsylvania State University. Finkelstein currently works as an Assistant U.S. Attorney with the U.S. Department of Justice in Philadelphia. Finkelstein serves as adjunct faculty of law at Drexel Law, Emory Law, and Rutgers Law and recently co-authored “Ethical Lawyering: A Guide for the Well-Intentioned” by Aspen Publishing.

cedures in place were reasonable. Discovery methods will not only be disclosed, but those methods will also be scrutinized with the benefit of hindsight. Discovery methods that appeared reasonable to the lawyer at that time they were used may be deemed unreasonable by the judge weeks, months, or years later. This can lead to embarrassment when a lawyer is “blamed” for having insufficient discovery methods in place to prevent waiver.

In contrast, with a non-waiver order in place there is no need for judicial review of discovery methods. The methods used are simply irrelevant. If information has been disclosed, that disclosure does not waive privilege regardless of the circumstances that led to the disclosure. Blame is irrelevant.

For these and other reasons, the Sedona Conference recommends the entry of a non-waiver order in every case. These orders offer clear benefits to the parties, with virtually no downside.

The Sedona Conference’s Recommendations

In addition to encouraging the use of non-waiver orders generally, the Sedona Conference offers several other recommendations to maximize the benefit of these orders. Three of those recommendations are highlighted and explained here.

First, consider moving for the entry of a non-waiver order even if the other parties do not consent. A court may enter a non-waiver order *sua sponte* or on motion by any party. If you are litigating against counsel who are unfamiliar with non-waiver orders or who are otherwise reticent to consider such an order—do not let this prevent you from moving for the entry of an order. Where the volume of discovery is significant, you should be able to articulate good cause for such an order to avoid the need to scrutinize in

detail each page of discovery before it is produced.

If you intend to move for a non-waiver order, do so early in the case. This helps you globally frame discovery in a way that is beneficial for your client. View the motion as an opportunity for you to educate the presiding judge about the volume of discovery and proportionality issues in your case. This may not only lead to the entry of a non-waiver order but also a more realistic discovery time-frames in the judge’s scheduling order.

Second, do not unnecessarily limit your non-waiver order. The text of Federal Rule 502(d) and New Jersey Rule 530(c)(4) are not limited to inadvertent disclosure. To the contrary, these rules apply to any disclosure. Yet lawyers are accustomed to discussing “inadvertent disclosure” and may use that term in their non-waiver orders. Avoid using the term “inadvertent disclosure” in your proposed order as doing so may encourage the court to apply the existing caselaw and to engage in a fact-specific analysis contrary to the intent of these rules. Instead, consider adopting the language of the model order promulgated by the Sedona Conference which states that the order applies to all disclosures “whether inadvertent or otherwise.” Using this language increases the odds that you will reap the full benefit of having a non-waiver order in place.

Third, research your jurisdiction to determine how broadly non-waiver orders are interpreted. Although the plain language of both the Federal Rules and New Jersey Rules limit the application of such an order to attorney-client privilege and work product, some courts have extended protection to other types of privilege.⁶ A non-waiver order can be even more powerful in such a jurisdiction. It can save you time and money spent on other types of privilege review in addition to a review for attorney-client

privilege and work product protected information.

Returning to the construction dispute at the beginning of this article, there would be clear benefits to using a non-waiver order in this litigation. With a non-waiver order in place prior to discovery commencing, there is no need to scrutinize every page of discovery. Instead, you can be confident in using keyword searches to screen for privilege because even if a page or two of privileged information slips through—you can claw it back without issue. You need not disclose your firm’s limited resources or the methods you used to conduct a privilege review—none of that is relevant.

By thinking ahead and taking advantage of the protection provided in the rules of evidence, you can save your client money and save yourself time to focus on other aspects of litigating the case. What once was a problem no longer is a problem. Retain privacy with non-waiver orders under either the New Jersey or Federal Rules of Evidence. ■

Endnotes

1. See Sedona Conference, The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production (2d ed. 2007).
2. The Sedona Conference, Commentary on the Effective Use of Federal Rule of Evidence 502(d) Orders, 23 SEDONA CONF. J. 1 (forthcoming 2022).
3. Fed. R. Evid. 502(d).
4. N.J.R.E. 530(c)(4).
5. Fed. R. Evid. 502(b).
6. The Sedona Conference highlights cases from Florida, California, and Alaska where courts more broadly interpreted the scope of a non-waiver order.



New Jersey State Bar Foundation

Medal of Honor Awards Dinner

*Honoring 2022
Medal of Honor Award Recipients*



Hon. Jaynee LaVecchia (Ret.)



Raymond M. Brown Esq.

**Tuesday, Sept. 20
5:30 p.m.**

**Park Chateau
East Brunswick**

Register now at moh.njsbf.org



Coordinating Care

Aligning 42 CFR Part 2 with HIPAA

Addressing privacy concerns for substance use disorder patients

By David N. Crapo

In 1972, Congress enacted 42 U.S.C. § 290dd-2 (“Part 2 Statute”), which generally prohibits federally supported substance use disorder (SUD) treatment programs (“Part 2 Programs”) and others lawfully in possession of SUD treatment information (“Lawful Holders”) from disclosing SUD treatment information to anyone without either the patient’s prior written consent or a court order. Enactment of the Part 2 Statute was triggered, in large part, by the reluctance of those suffering from SUDs to seek treatment because of (i) the stigma attached to SUDs; (ii) discrimination resulting from the disclosure of SUD information; and (iii) the potential use of SUD treatment information in criminal prosecutions. In 1975, the Substance Abuse and Mental Health Services Administration (SAMHSA) promulgated the Confidentiality of Substance Use Patient Records Regulations (“Part 2”) at 42 CFR Part 2 to implement the Part 2 Statute. Reflecting the significant risks to the patient inherent in the disclosure of SUD treatment information, Part 2’s restrictions are more stringent than the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which was promulgated in 2003 and more generally regulates the privacy of health care treatment records.¹

For many reasons, people with SUDs often suffer from one or more comorbidities. Patients suffering from multiple medical conditions are best served by coordination between their health care providers. For that reason, tension has arisen between the well-intentioned—and crucial—protections

embodied in Part 2 and the urgent need to coordinate the treatment of a patient’s SUDs with the treatment of comorbidities. Indeed, many health care providers found Part 2 to impede care coordination. It should come as no surprise, therefore, that the inconsistencies between Part 2 and the more flexible HIPAA Privacy Rule became increasingly evident over time.

The opioid crisis and the COVID-19 emergency increased the need to facilitate the coordination between SUD treatment and the treatment of comorbidities. The Coronavirus Aid, Relief, and Economic Security (CARES) Act,² which was enacted on March 27, 2020, amended the Part 2 Statute to more closely align it with the HIPAA Privacy Rule. Those amendments (“Part 2 Statute Amendments”) expand the ability of Part 2 Programs and Lawful Holders to disclose SUD treatment records with the patient’s non-SUD health care providers for treatment, payment, and health care operations purposes. Balancing the relaxation of the disclosure restrictions, the amendments do not lift the requirement that the SUD patient must initially consent to that sharing, and Part 2 now subjects Part 2 Programs and Lawful Holders to HIPAA’s Breach Notification Rule. In sum, the Part 2 Statute Amendments balance the relaxation of Part 2’s disclosure restrictions to facilitate health care coordination with the continued—and crucial—need to maintain the privacy of that information.

Initially, Part 2 required either a separate patient consent for each use or disclosure of SUD treatment information or the

identification in the consent of each **individual** entitled to use or disclose such information. The Part 2 Statute Amendments permit the use of a general consent executed by the patient. Upon the patient's execution of a general consent, SUD treatment records "may be used or disclosed by a covered entity, a business associate of the covered entity or another business associate for...treatment, payment and healthcare operations as permitted by the HIPAA regulations."³ Consistent with the HIPAA Privacy Rule, disclosures of SUD treatment are limited to what is minimally necessary to achieve the purpose for which disclosures are made.⁴

Redisclosure of SUD treatment information is permitted under a general consent, but only for treatment, payment, and health care operations.⁵ It is, therefore likely that the more stringent Part 2 limitations no longer apply to such redisclosures. However, as with HIPAA, more stringent state laws will control the redisclosure of SUD treatment information. Also, as with HIPAA, the patient may revoke a general consent (in writing) at any time, although the revocation will not impact prior disclosures and redisclosures.⁶



DAVID N. CRAPO is of Counsel to Gibbons P.C. at its Newark office and is a member of the firm's Financial Restructuring and Creditors' Rights Group, Health Care Team, and Data Privacy and Security Team. He has served as a patient care ombudsman in the bankruptcy cases of several behavioral health care providers.

The Part 2 Statute Amendments address SUD patients' fears of the use of SUD treatment information against them in administrative or judicial proceedings (especially criminal prosecutions) by tightening the rules regarding the use of SUD treatment information or testimony containing such information in such pro-

The Part 2 Statute Amendments address SUD patients' fears of the use of SUD treatment information against them in administrative or judicial proceedings (especially criminal prosecutions) by tightening the rules regarding the use of SUD treatment information or testimony containing such information in such proceedings.

ceedings. The Part 2 Statute Amendments continue the general rule under Part 2 of prohibiting the use of SUD treatment information or testimony absent prior patient consent or a court order authorizing such use.⁷ Because the use of SUD information in an administrative or judicial procedure would not likely constitute a treatment, payment, or health care operations use, a specific consent by the patient would almost certainly be neces-

sary. Additionally, such information or testimony: (i) may not be entered into evidence in any state or federal civil action or criminal prosecution; (ii) shall not form a part of the record for decision or otherwise be considered in any proceeding before a federal, state, or local agency; (iii) shall not be used by any federal, state, or local agency for a law enforcement purpose or to conduct any law enforcement investigation; and (iv) shall not be used in any application for a warrant.⁸

The Part 2 Statute Amendments also address the fear of discrimination that discouraged those suffering from SUDs from seeking treatment. Recipients of SUD treatment information are prohibited from discriminating against the patient with respect to: (i) access to health care treatment; (ii) hiring, firing, terms of employment, or workers compensation; (iii) sale, rental, or continued rental of housing, (iv) access to federal, state, or local courts; or (v) access to government-provided social services or benefits.⁹ Recipients of federal funding are singled out for special attention. They may not discriminate against individuals with respect to access to the federally-funded services they provide on the basis of SUD treatment information they have received concerning those individuals.¹⁰ Whether the receipt of the SUD treatment information is intentional or inadvertent is immaterial to the federal funds recipients' obligations to comply with the non-discrimination prohibition of the Part 2 Statute Amendments.

As part of the alignment of Part 2 with HIPAA, the Part 2 Statute Amendments incorporate several HIPAA provisions into Part 2. The HIPAA Breach Notification Rule is one of those provisions.¹¹ That rule requires HIPAA-covered entities (*i.e.*, health care providers, health plans, and health care clearing houses) to report breaches of protected health information as soon as possible, but no more

than 60 days after becoming aware of the breach.¹² The rule also sets forth extensive requirements governing the content, form, and procedures relating to a breach notification, including a risk analysis that must be conducted to determine whether an authorized use or disclosure of SUD treatment information constitutes a reportable breach. The rule's requirements, therefore, apply to those Part 2 programs and Lawful Holders not already subject to them.

The Part 2 Statute Amendments permit the disclosure of SUD treatment information to public health authorities, as long as the information is de-identified in a manner consistent with HIPAA's de-identification standards.¹³ For purposes of HIPAA, de-identification requires the removal of certain identifiers or the use of an actuarial method of de-identification.¹⁴

SUD patients are now entitled to an accounting of the disclosures of their SUD treatment information pursuant to a general consent for treatment, payment, or health care operations.¹⁵

Violations of Part 2 as amended are now subject to the same penalty structure applicable to HIPAA violations.¹⁶ HIPAA provides a tiered approach to the penalties grounded in the culpability of the violator.¹⁷ The four tiers and their respective current penalty amounts are:

- **Tier 1:** The violator lacked knowledge of the violation, could not have realistically avoided it, and had taken a reasonable amount of care to comply with HIPAA Rules. For violations in this tier, the minimum fine is \$120 per violation up to a maximum fine of \$30,113 per violation, with a maximum fine of \$30,113 per year for each type of violation.
- **Tier 2:** A violation of which the covered entity should have been aware but could not have avoided even with a reasonable amount of care, falling

short of willful neglect of the Part 2 and HIPAA Rules. For violations in this tier, the minimum fine is \$1,205 per violation up to a maximum fine of \$60,226 per violation, with a maximum fine of \$120,452 per year for each type of violation.

- **Tier 3:** A violation suffered as a direct result of "willful neglect" of the Part 2 and HIPAA Rules, in cases where an attempt has been made to correct the

The Part 2 Statute Amendments permit the disclosure of SUD treatment information to public health authorities, as long as the information is de-identified in a manner consistent with HIPAA's de-identification standards.

violation. For violations in this tier, the minimum fine is \$12,045 per violation up to a maximum fine of \$60,226 per violation, with a maximum fine of \$301,130 per year for each type of violation.

- **Tier 4:** A violation of Part 2 and HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation within 30 days of discovery. For violations in this tier, the minimum fine is \$60,226 per violation up to a maximum fine of \$1,806,775 per violation, with a maxi-

mum fine of \$1,806,775 per year for each type of violation.

Following the enactment of the Part 2 Statute Amendments, SAMHSA issued a rule ("Transitional Rule") amending Part 2¹⁸ to facilitate the coordination of health care for SUD patients. The Transitional Rule became effective on Aug. 20, 2020. It sets interim standards to be used pending the issuance of a final rule implementing the Part 2 Statute Amendments. Its purpose is not to implement the Part 2 Statute Amendments.

One focus of the Transitional Rule is to facilitate the coordination between Part 2 Programs and non-Part 2 health care providers. One obstacle to such coordination was the potential that the inclusion of SUD treatment records in a medical file could convert a non-Part 2 provider's records into Part 2 records subject to Part 2 Restrictions. The Transitional Rule provides that treatment records created by a non-Part 2 provider based on the provider's own patient encounter(s) are explicitly not covered by Part 2, even if they have received the information orally from a Part 2 Program or Lawful Holder.¹⁹ However, if a non-Part 2 provider receives any written SUD treatment records from a Part 2 Program and incorporates those records into non-Part 2 records, the non-Part 2 records will be subject to Part 2's restrictions.²⁰ Consequently, written records received from Part 2 Programs be segregated from non-Part 2 records to ensure that new records created by non-Part 2 providers will not become subject to Part 2.²¹

Consistent with the policies underlying the Part 2 Regulations, only limited exceptions were permitted to the general prohibition against disclosure of SUD treatment information. The Transitional Rule relaxed some of those exceptions. In response to the COVID-19 emergency, for example, the medical emergency

exception was amended to permit disclosure of SUD treatment information without prior patient consent if: (i) a federal or state authority declares a state of emergency arising out of a natural or major disaster; (ii) the operations of the Part 2 Program are suspended; and (iii) the Part 2 Program cannot obtain informed patient consent.²² This expanded disclosure authorization terminates, however, once the Part 2 Program again becomes operational.²³

The Transitional Rule aligns Part 2's research exception more closely with the HIPAA Privacy Rule and the Common Rule for research on human subjects. Part 2 Programs and Lawful Holders may disclose patient-identifying SUD treatment information to qualified research personnel if: (i) the researcher is subject to and documents its compliance with privacy protections for human research subjects contained in the Common Rule (at 45 CFR §§ 46.111, 46.116) or the HIPAA Privacy Rule (at 45 CFR 164.512(i)); or (ii) if the researcher has not documented compliance with either HIPAA or the Common Rule, the disclosure complies with the provisions of § 512(i) of HIPAA Privacy Rule.²⁴ However, only aggregated or de-identified data may be used in research reports.²⁵ Researchers must also agree to resist judicial proceedings attempting to obtain access to the SUD treatment information.²⁶

The Transitional Rule amends sub-sections (c), (f), and (g) of § 2.53 of Part 2, which implements the audit/evaluation exception restrictions, to include audits concerning: (i) changing policies to improve patient outcomes across Part 2 Programs; and (ii) determining the need to adjust payment policies. Only de-identified data should be used for an audit or evaluation. Patient-identifying data may be disclosed to federal, state, or local government agencies in connection with an audit required by law if the audit cannot

be carried out without de-identified data. SAMHSA urges parties to use de-identified data for such disclosures but recognizes that doing so may not be cost-effective or may be too cumbersome.

In response to the opioid crisis, section 2.34 of Part 2 now permits Central Registries to disclose SUD treatment information to all providers, not only opioid use treatment providers, including whether a patient is already receiving opioid use treatment. This amendment prevents duplicative enrollment in such treatment programs and informs treatment providers' decisions concerning prescription and plans of care. Also, in response to the opioid crisis, the Transitional Rule adds § 2.36 to Part 2, authorizing opioid treatment providers and other Lawful Holders to enroll in and, with the patient's consent, disclose prescription information to state Prescription Drug Monitoring Programs.

The Transitional Rule amends § 2.31(a)(4) of Part 2 to move it toward the general consent authorized by the Part 2 Statute Amendments. The amendment generally eliminates the requirement that a patient's consent to disclosure identify the individual or individuals to whom SUD treatment is being disclosed. In most cases, a valid consent need identify only either the individuals or the entities to which the disclosure is being made. The amendment provides patients with options on how SUD treatment information is disclosed and facilitates the coordination of care. The amendment does not, however, completely eliminate the requirement that each individual to whom SUD treatment information is being disclosed be identified in the consent. Amended § 2.31(a)(4) retains a limited requirement concerning the identification of individuals receiving such information in connection with disclosures for research purposes or to health information exchanges. It

remains to be seen whether the anticipated final rule eliminates this limited requirement.

The Transitional Rule amends §2.13 of Part 2 to provide the patient with a right of accounting of the disclosures of SUD treatment information pursuant to a general consent during the two years immediately preceding the request for an accounting, which is not as broad as the accounting right provided by HIPAA Privacy Rule, which has been incorporated into the Part 2 Statute. In response to certain formatting limitations in electronic health records, § 2.32 of Part 2 has been amended to approve the use of a shortened version of the notice to the recipient of SUD treatment information that re-disclosure prohibited. SAMHSA encourages the use of the longer notice where possible. The Transitional Rule amends § 2.33(b) of Part 2, which permits disclosures for payment and health care operations to expressly include disclosures for care coordination and case management, but only if the patient consent has consented to such uses.

To encourage patients suffering from SUDs to seek treatment without fear of prosecution, by court order, § 2.17 of Part 2 generally prohibits placing undercover agents or informers in Part 2 Programs. Section 2.67(b) and (e) of Part 2 limits the use of undercover agents to investigations of the Part 2 Program itself, its employees, or agents for serious illegal conduct and cannot be used to investigate patients. Amended § 2.67(d)(2) expands the duration of the agent's placement to 12 months, but requires a new court order for an agent to remain in place beyond the 12-month period.

Part 2 generally requires a Part 2 Program to communicate with and receive communications only via a Part 2-authorized medium. Personal devices and cell phone accounts used in such communications must be sanitized of any SUD

treatment information. Before the promulgation of the Transitional Rule, it was unclear whether this required the sanitization of the whole device. In guidance on the Transitional Rule, SAMHSA has stated that media and accounts may be sanitized by immediately deleting the SUD treatment information.²⁷ Any response to a patient should be on an authorized medium, unless response by a personal account is in the patient's best interest.

As noted above, the Transitional Rule does not implement the Part 2 Statute Amendment. It does, however, align Part 2 more closely to HIPAA and makes significant progress toward the availability of a general consent. A final rule fully implementing the Part 2 Statute Amendments was supposed to have been promulgated by mid-2021. Promulgation has been delayed several times, and the final

rule has still not been issued for comment, let alone promulgated. Hence, Part 2 Programs, Lawful Holders, and their counsel will be governed by the Transitional Rule to the extent it is consistent with the Part 2 Statute Amendments for the foreseeable future. ■

Endnotes

1. See 45 CFR §§ 164.500, et seq.
2. Pub. L. No. 116-136, congress.gov/bill/116thcongress/ho-use-bill/748/text
3. 42 U.S.C. § 290dd-2(b)(1)(B)
4. *Id.*
5. 42 U.S.C. § 290dd-2(b)(1)(B)
6. 42 U.S.C. § 290dd-2(b)(1)(C)
7. 42 U.S.C. § 290dd-2(c)
8. 42 U.S.C. § 290dd-2(c)(1)-(4)
9. 42 U.S.C. § 290dd-2(i)(1)
10. 42 U.S.C. § 290dd-2(i)(2)
11. 42 U.S.C. § 290dd-2(j)
12. 45 CFR 164.400, et seq.
13. 42 U.S.C. § 290dd-2(i)(2)
14. See 45 CFR § 164.514(b)(2)(D)
15. 42 U.S.C. § 290dd-2(b)(1)(D)
16. 42 U.S.C. § 290dd-2(f)
17. 45 CFR § 160.404
18. 42 CFR §§ 2.1, et seq.
19. 42 CFR § 2.12(d)(2)(ii)
20. *Id.*
21. *Id.*
22. 42 CFR § 2.51(a)(2)
23. *Id.*
24. 42 CFR § 2.52(a)(1) and (2)
25. 42 CFR § 2.52(b)(3)
26. 42 CFR § 2.52(b)(1)
27. See Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule accessed on March 15, 2022 at samhsa.gov/newsroom/press-announcements/202007131330.



THE NATIONAL ACADEMY OF DISTINGUISHED NEUTRALS

America's Premier Civil-Trial Mediators & Arbitrators Online

NADN is proud to partner with the National Defense and Trial Bar Associations



dri™

The Voice of the **Defense** Bar



AMERICAN
ASSOCIATION FOR
JUSTICE®

The Association for Trial Lawyers

2022 Trial Advertiser

View Bios & Availability Calendars for the top-rated neutrals in each state, as approved by local litigators

www.NADN.org

The National Academy of Distinguished Neutrals is an invitation-only professional association of over 1000 litigator-rated mediators & arbitrators throughout the USA, including over 30 members of our New Jersey Chapter. For local ADR professionals, please visit www.NJMediators.org



Commercialization of Your DNA

*Privacy Regulations Lagging for
Companies Collecting Genetic Data*

By Jayla E. Harvey

There are many legal concerns regarding genetic privacy in the wake of direct-to-consumer genetic testing. Major gaps in privacy regulations exist for genomic data, which have essentially given DNA-test companies unfettered discretion to sell the data they collect from their customers. This has resulted in increasing privacy risks, with a growing concern that technology companies may abusively monetize data.¹

Companies that conduct direct-to-consumer genetic testing (DTC GT) charge consumers to sequence their DNA, but then they store the sequenced DNA samples and sell the DNA sequences in bulk to third-party research companies. Approximately 30 million people have taken and submitted an at-home DNA test,² yet few realize that when they submit their DNA sample to DTC GT companies, they have just paid someone to take the “most valuable thing they own.”³ —That is, their full genetic code. Genes disclose information relating to health, personality traits, family history, and information about relatives, and when this information is placed in the wrong hands, it bears the risk of abuse and irreparable harm.⁴

The risks associated with genetic data are heightened relative to other consumer data or health data because of the exceptional nature of genetic information.⁵ DNA does far more than merely identify a person: “DNA stores and reveals massive amounts of personal, private data about that individual [and persons related to them], and the advance of science promises to make stored DNA only more revealing in time.”⁶ In 2018, a study purported it would be possible to identify nearly any individual in a certain ances-

tral group using a genetic database that includes information about 2% of that population, regardless of whether that individual participated in consumer genetic testing.⁷ This means that it is currently possible to identify just about every American of European descent by their DNA alone by using open DNA databases to generate gene maps of distant cousins.⁸ Given the trajectory of the DTC GT industry and quickly evolving investigative technology, it soon may be possible that everyone could be identified and tracked by the government even if they have never completed a genetic test.⁹

A real-life example of what this study forewarned is a 2018 law enforcement genealogy database that was used to track down the Golden State Killer by using DNA from a cold murder case to identify his great-great-great-grandparents.¹⁰ Typically, the Fourth Amendment’s protections against unreasonable searches and seizures would prevent government use of individuals’ genetic material without a proper warrant.¹¹ But when the information comes from DTC GT companies, the government can invoke the “third-party doctrine,” which allows it to obtain data without a warrant when a suspect has voluntarily given that data to a third party.¹² Although, the suspect did not volunteer that information, a very distant relative did.¹³ This case also demonstrated that genealogical

matches are not perfect. Before police arrested the now-convicted Golden State Killer, they incorrectly identified a bedridden man in Oregon as a genetic match.¹⁴

Beyond improper access to law enforcement, once a consumer submits a biological sample, they have little control over who can get their hands on it in the future. Quite simply, our legal framework does not reach what DTC GT companies do with the genetic information they collect.¹⁵ DTC GT companies have essentially removed the health care industry as a gatekeeper for genetic



JAYLA E. HARVEY is newly admitted attorney at Lerner David Littenberg Krumholz & Mentlik in Cranford. Her practice focuses on intellectual property law, namely patent litigation and prosecution. Jayla has a B.S. in biology with a minor in chemistry and worked as a research assistant in a computational biology lab that focused on tracking the evolutionary history of various genetic traits. During law school, Jayla was a clinical law student in the Intellectual Property Law Clinic at Rutgers Law School.

testing.¹⁶ As medical professionals are taken out of the equation, so are the legal safeguards implemented to protect patients' privacy. Current health privacy laws, namely Health Insurance Portability and Accountability Act (HIPAA) and Genetic Information Nondiscrimination Act (GINA), fail to address the unique privacy concerns raised by the actions of DTC GT companies, like re-identification of anonymized data samples or nonconsensual use of DNA.

HIPAA, which was designed to protect patient privacy, does not apply to DTC GT companies.¹⁷ HIPAA rules prohibit covered entities and their business associates from using or disclosing protected health information,¹⁸ where "covered entities" is defined "as a health plan, health care clearinghouse, or health care provider."¹⁹ This definition does not reach the DTC GT industry as they are viewed as wholly outside the medical field. Even if this definition were stretched to include DTC GT companies, HIPAA would fail to offer more privacy protection than what is currently offered by the industry. Industry leaders rely on de-identification and aggregation of data to sidestep potential regulations.²⁰ And under HIPAA's privacy rule, de-identified information requires no privacy protections and is not covered, even though DNA is inherently identifiable.²¹

Similarly, GINA was enacted in 2008 to protect individuals from employment or health insurance discrimination based on their genetic information.²² GINA prohibits employers and health insurers from requesting or accessing "confidential medical record[s]."²³ Again, DTC GT companies fall outside the scope of this legislation. And even if GINA was extended to the DTC GT industry, it is confined to prohibiting the use of genetic information for discriminatory purposes and does not reach any of the enumerated privacy concerns associated with this industry.²⁴ The act does not touch on preventing the oversharing of

genetic information beyond the primary purpose for which it was collected to unauthorized third parties. Nor does the act address how to effectively guard an individual's identity once shared.

Genetic testing companies promise not to sell or give away data without consent, but that consent is usually a very broad blanket statement that is included in an initial contract few consumers read thoroughly or fully comprehend, leaving the companies to use the DNA sample however they wish.²⁵ DTC GT giant Ancestry.com grants itself broad licensing rights to the user's genetic results in its terms and conditions.²⁶ While this broad licensing language is commonplace in many terms and conditions, this has substantially different implications when it comes to your DNA.

DNA is a valuable research commodity and is essential to shift our health care system into a personalized medicine model. Researchers' access to large and diverse databases is crucial in developing health treatments.²⁷ However, we cannot ignore the privacy concerns that arise when private companies are allowed to freely trade genetic information on the open market. The DTC GT has become a multi-billion-dollar industry that is fueled by the genetic information it collects.²⁸

There is a need for laws to allow individuals to retain substantial control over their genome beyond the promise of hollow anonymity. DTC GT companies have changed the way people access this highly personal information, and the law needs to change to address gaps created by this shift. ■

This article first appeared in the Winter 2022 Dictum, published by the NJSBA Young Lawyers Division, and is reprinted here with permission.

Endnotes

1. *The Social Dilemma*, Netflix.
2. Rani Molla, *Why DNA tests are*

suddenly so unpopular, Vox (Feb. 13, 2020), [vox.com/recode/2020/2/13/21129177/consumer-dna-tests-23andme-ancestry-sales-decline](https://www.vox.com/recode/2020/2/13/21129177/consumer-dna-tests-23andme-ancestry-sales-decline).

3. Shanna Manson, *Comments: Privacy of Information and DNA Testing Kits*, 27 Cath. U. J. L. & Tech. 161, 164 (2018) (quoting Peter Pitts of the Center of Medicine in the Public Interest).
4. Manson, 27 Cath. U. J. L. & Tech. at 164.
5. Samuel A. Garner & Jiyeon Kim, *Article: The Privacy Risks Of Direct-To-Consumer Genetic Testing: A Case Study Of 23 Andme And Ancestry* Wash. U.L. Rev. 1219, 1224 (2019).
6. *United States v. Kincaid*, 379 F.3d 813, 842 n.3 (9th Cir. 2004) (Gould, J., concurring).
7. Jamie Ducharme, *Millions of Americans Could Be Identified Using Consumer Genetic Databases—Even If They've Never Taken a DNA Test*, Time (Oct. 12, 2018, 3:49PM), time.com/5423170/dna-test-identify-millions/.
8. Megan Molt, *The US urgently needs new genetic privacy laws*, WIRED.com (May 1, 2019, 8 a.m.), [wired.com/story/the-us-urgently-needs-new-genetic-privacy-laws/](https://www.wired.com/story/the-us-urgently-needs-new-genetic-privacy-laws/).
9. Rasheed, 2020 U. Ill. L. Rev. at 1250.
10. Justin Jouvenal, *To Find Alleged Golden State Killer, Investigators First Found His Great-Great-Great-Grandparents*, Wash. Post (April 30, 2018, 5:22 PM), [washingtonpost.com/local/public-safety/to-find-alleged-golden-state-killer-investigators-first-found-his-great-great-great-grandparents/2018/04/30/3c865fe7-dfcc-4a0e-b6b2-0bec548d501f_story.html](https://www.washingtonpost.com/local/public-safety/to-find-alleged-golden-state-killer-investigators-first-found-his-great-great-great-grandparents/2018/04/30/3c865fe7-dfcc-4a0e-b6b2-0bec548d501f_story.html).
11. Ayesha K. Rasheed, *Article: Personal Genetic Testing and the Fourth Amendment*, 2020 U. Ill. L. Rev. 1249, 1250 (2020).
12. *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).
13. Jouvenal. *To Find Alleged Golden State*

Killer, Investigators found His Great-Great-Grandparents.

14. Michael Balsamo et al., *Police Using Genetic Sites Misidentified Oregon Man as Golden State Serial Killer Suspect in 2017*, Chi. Trib. (Apr. 28, 2018, 9:39 AM), chicagotribune.com/news/nationworld/ct-genealogy-site-serial-killer-20180427-story.html.
15. Gabrielle Kohlmeier, *Article: The Risky Business of Lifestyle Genetic Testing: Protecting Against Harmful Disclosure of Genetic Information*, UCLA J.L. & Tech. 5, 10 (2007).
16. Garner & Kim, 96 Wash. U. L. Rev. at 1236.
17. 45 C.F.R. § 164.502 (2021).
18. 45 C.F.R. § 164.502(a) (2021).
19. 45 C.F.R. § 160.103 (2021).
20. Benjamin T. van Meter, *Note: Demanding Trust in the Private Genetic Data Market*, 105 Cornell L. Rev. 1527, 1531 (2020).

21. Stephen B. Thacker, *HIPAA Privacy Rule and Public Health Guidance from CDC and the U.S. Department of Health and Human Services*, CDC (Apr. 3, 2003), cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm#:~:text=The%20Privacy%20Rule%20protects%20certain%20information%20that%20covered,electronic%20media%20or%20any%20other%20form%20or%20medium.
22. Genetic Information Nondiscrimination Act § 2(5), 122 Stat. at 881-82.
23. 42 U.S.C. § 2000ff-5(a) and (b).
24. Garner & Kim, 96 Wash. U. L. Rev. at 1227-28.
25. Manson, 27 Cath. U. J. L. & Tech. at 164.
26. Manson, 27 Cath. U. J. L. & Tech. at 165-66 “[B]y submitting User Provided Content through any of the Services, you grant Ancestry a

sublicensable, worldwide, royalty-free license to host, store, copy, publish, distribute, provide access to, create derivative works of, and otherwise use such User Provided Content to the extent and in the form or context we deem appropriate on or through any media or medium and with any technology or devices now known or hereafter developed or discovered”

27. Kristen V. Brown, *These Companies want you to sell your DNA on the Internet*, Gizmodo (January 18, 2018 2:05PM), gizmodo.com/should-you-sell-your-dna-on-the-internet-1822117457.
28. Kristen V. Brown, *23andMe is selling your data but not in the way you think*, Gizmodo (April 14, 2017), gizmodo.com/23andme-is-selling-your-data-but-not-how-you-think-1794340474.

EXCELLENCE IN CLE Awards Reception

Monday, Sept. 12 | 6 p.m. | New Jersey Law Center | **FREE** registration

Honoring

2020 ALFRED C. CLAPP AWARD RECIPIENT

Gianfranco Pietrafesa

2021 ALFRED C. CLAPP AWARD RECIPIENT

Christopher Placitella

**2020 DISTINGUISHED SERVICE
AWARD RECIPIENTS**

**Hon. Lisa James-Beavers, JSC
Anne S. Babineau
John F. DeBartolo
Robyn B. Gigl**

**2021 DISTINGUISHED SERVICE
AWARD RECIPIENTS**

**Hon. Sohail Mohammed, P.J.Cr.
Robert Brass
Crystal West Edwards
Tracey Goldstein**

REGISTER
NOW AT
njicle.com

Dragging **DARK** PATTERNS into the Light

Recognizing and Mitigating the Pervasive Risk of Manipulative Interface Design for Clients in the Digital World

By Alfred R. Brunetti

Allow us to access your contacts and friends so that you can access this app's full suite of features. To cancel your subscription, simply click through this series of prompts (and then call our customer service department to confirm your choice). Are you sure you don't want us to tell you about special limited-time offers that will save you money?

The printed word in a periodical may never be as visually appealing or engrossing as the online and mobile interfaces that have become the increasingly predominant way most of us interact with the larger world. But, even through this compromised medium of ink and glossy paper, you can likely feel the above statements' subtle yet intentional manipulation achieved by presenting heavily-weighted options via deliberate phrasing, pre-selected answers and convoluted constructs that strategically—and psychologically—constrict your range of responsive choices to result in a designed choice architecture.¹ These types of purposeful manipulations and subversions, when appearing in the user experience (UX) design of a digital interface, have become known as Dark Patterns.

Clients may be deploying these dubious design elements on their websites, apps and/or social media platforms without appreciating the growing risk of doing so. This article addresses the issue, provides an update on various applicable laws, and offers some practical tips for managing client risk while still satisfying client objectives.

What are Dark Patterns?

Although there is currently no standardized single definition, privacy practitioners generally define Dark Patterns as user interface design choices that benefit designers by coercing, manipulating and/or tricking the user into making decisions, which are contrary to the user's initial intentions or to the user's detriment.² The term Dark Patterns was first coined by a renowned UX expert more than a decade ago³ and has

since grown to encompass and describe a veritable smorgasbord of deceptive or manipulative interface design features all structured to bend the user's autonomy toward the designer's objective.⁴ The perplexing thing about a concept as amorphous as Dark Patterns is that its manifestations are limited only by the creativity of its designers.⁵ Perhaps because of their chameleon-like nature, Dark Patterns can be found in virtually any form of digital user interface and have become an especially troubling feature in the online expanses of retail, data privacy and even gaming.

To liberally paraphrase Justice Stewart,⁶ you will often kind of know them when you see them and, if you have been online at any point this millennia, you have very likely encountered Dark Patterns in spades. In fact, Dark Patterns have so deeply infiltrated the online UX and spread throughout the interface design universe that experts have begun to parse out their various forms into general categories. Though there exists no bright-line measure to identify the presence of a Dark Pattern, ongoing industry observation and scholarship have arrived on a loose taxonomy of more than a dozen different types⁷ of Dark Patterns that can be broken down into interchangeable groupings found in both retail and user privacy contexts alike. Because all Dark Patterns purposefully impact the constructed Choice Architecture⁸ experienced by users online, the way in which such a defined environment is altered by a specific Dark Pattern serves as a convenient dividing line by which to separate the two main ways in which Dark Patterns work: either by modifying the decision space itself or by manipulating the flow of information into that decision space.⁹

The ever-growing taxonomy of identified Dark Pattern types includes:

- The **Bait & Switch**,¹⁰ perhaps the epitome of underhanded sales practices

where a customer-selected item is switched out for a less desirable or more expensive item during the sale transaction;

- **Hidden Costs**,¹¹ a tried-and-true deceitful practice where additional costs or fees are tallied onto the total sale price just before or at the final stage of the purchase;
- **Basket Sneak**,¹² a cousin of the Hidden Costs where a pre-checked box or opt-in toggle automatically slips in an additional item or service to a purchase unless the consumer catches the add-on and manually makes a change;
- **Price Comparison Prevention**,¹³ the use of a purposefully convoluted navigation or an intentionally vague descriptive to prevent a true apples-to-apples comparison of a product;
- **Forced Continuity**,¹⁴ where upon the ending of a trial or discounted price period, a new subscription period or more retailer-friendly terms snap into effect without proper notice to the consumer or in a manner which makes it unreasonably burdensome for the consumer to prevent the continuity;
- **Roach Motel**,¹⁵ a manifestation hallmarked by a welcoming design that facilitates easy user access or registration but which couples that easy introduction with a needlessly complicated or obtuse design or navigation pathway intended to frustrate any user attempts to leave the service or terminate a subscription;
- **Misdirection**,¹⁶ blurring the line between promotion and deception, this design element purposefully pulls the user's attention away from an option or decision path that would not benefit the designer and may even employ visual interference and low-prominent text to do so;
- **Trick Questions**,¹⁷ antithetical to clear and simple, these queries prey upon a

user's typical expectations and use intentionally transposed context, double negatives or similar grammatical twists to trick the user into providing answers for the designer's benefit;

- **Oversharing**,¹⁸ by a similar contrivance of context and grammar, this form goads the user to provide more information than necessary to accomplish the transaction, e.g. requesting your telephone number and prior address to register for email updates;
- **Friend Spam**,¹⁹ in the vein of Oversharing, this manifestation pressures or incentivizes the user to provide access to their contact's identifiers;
- **Confirmshaming**,²⁰ presenting an option in a manner that guilties the user into reconsidering and altering the user's original intentions; e.g. 'Are you sure you don't want to protect your family vacation with this iron-clad travel insurance?';
- and **Designed Advertisements**,²¹ the practice of fully incorporating sponsored content into required navigation steps or presenting the ads themselves as direct content.

Building upon these original groupings, researchers have recently named additional commonly found categories which include:



ALFRED R. BRUNETTI is a partner at McElroy, Deutsch, Mulvaney & Carpenter, LLP and a Certified Information Privacy Professional in the laws of the United States (CIPP/US). His practice focuses upon complex commercial litigation and counseling on privacy, data management and corporate compliance matters.

- **Nagging**,²² when a user's intended task is interrupted by other tasks not directly related to the intended task;
- **Forced Action**,²³ when a user is made to perform a specific action to access, or to continue to access, a desired functionality;
- **Misrepresenting**,²⁴ when ambiguous or outright incorrect information is presented to purposefully trick the user; and
- **Controlling**,²⁵ where the designer interrupts a user's task flow and redirects them to the designer's own task flow.

Regardless of the names or stripes, a Dark Pattern's goal is consistently simple: to manipulate or outright deceive the user—typically at a decision point—into making a choice or taking an action that benefits the designer, not the user.²⁶ In the retail space, that can mean making a purchase or selection that was not initially intended, but in the data privacy space, that typically results in a user sharing more data or authorizing the use of certain data beyond what the user would have initially, or freely, intended. A survey of suspected Dark Pattern sightings that have been reported to researcher-maintained tip lines and sites²⁷ reveals that online interfaces of all sizes and types, from many of the world's most recognizable platforms to much more obscure apps, have been flagged by concerned individuals for the use of suspected Dark Patterns. But it is not just leery consumers who have taken notice.

How are Dark Patterns Being Regulated?

Despite the increased attention by academics and regulators on manipulative design practices, precious little exists in the form of statutes or regulations expressly banning the use of Dark Patterns by name; however, to fill that void, both state and federal authorities have begun to take notable action.

At the Federal Level:

In the continuing absence of a comprehensive federal privacy statute,²⁸ in recent years via a series of settlements against online businesses,²⁹ the Federal Trade Commission has systematically begun to address and regulate Dark Patterns in the marketplace. The FTC hosted a public workshop in April 2021 entitled, “Bringing Dark Patterns to Light,” to analyze digital Dark Patterns and to put both industry and the public on notice of the prevalence of manipulative design practices in websites and mobile applications.³⁰ In October 2021, the FTC loudly announced that it would “[r]amp up [e]nforcement against [i]llegal Dark Patterns” by releasing a detailed enforcement policy statement focused upon subscription continuity-type Dark Patterns and emphasizing the enforcement points of disclosure, consent and easy cancellation previously established by the FTC's existing rules and settlements.³¹ Even the retail behemoth Amazon is not exempt from the FTC's increasing enforcement focus. It has been widely reported that the FTC continues to investigate Amazon's use of supposed Dark Patterns in its Amazon Prime membership subscriptions³² and its recognized practice of automatically enrolling consumers into a 30-day free trial of Amazon Prime with a single-click before eventually rolling that membership into a recurring annual subscription.³³

Based on its developing track record, it appears unlikely that the FTC will discontinue its ambitious enforcement activities against Dark Patterns any time soon. Instead, in the ongoing absence of a manipulative design-specific federal law, it is likely that the FTC will continue to exercise its Section 5 authority³⁴ to combat Dark Patterns practices especially when they appear in the retail space.³⁵

At the State Level:

California³⁶ became impatient awaiting movement on the federal privacy

front and took action in 2018 by passing the California Consumer Privacy Act of 2018 (CCPA), a comprehensive data privacy statute. The CCPA broke new ground by affording California residents various enumerated rights concerning the collection and use of their personal information by private industry.³⁷ In March 2021, only 15 months after it became effective, the CCPA was amended to squarely address areas where Dark Patterns commonly proliferate: opt-out decision points where a user has to choose whether to permit the sale or use of personal information. Without explicitly naming or defining Dark Patterns, the amended CCPA prohibits a business from using “a method that is designed with the purpose of having a substantial effect of subverting or impairing a consumer's choice to opt-out” of the use of personal information and requires that a business's methods for submitting requests to opt-out be “easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out.”³⁸

Unsatisfied, California again took action by passing the California Privacy Rights Act of 2020 (CPRA), which significantly amends and expands the CCPA.³⁹ With an effective date of January 1, 2023, the CPRA will be the first state statute in the nation to expressly define Dark Patterns and provides for a two-prong attack on manipulative designs: by definition and by nullification. The CPRA defines Dark Patterns as “[a] user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation,”⁴⁰ and it codifies that any “agreement obtained through use of dark patterns does not constitute consent.”⁴¹ The statute's formal rulemaking process began in July 2022 but the final rules—expected to be issued, at the earliest, only weeks before the CPRA's Jan. 1, 2023, effective date⁴²—will likely identify specific Dark Pattern manifestations and

expressly clarify that a design feature can be a Dark Pattern regardless of the designer's intent.

Following loosely on the heels of the CPRA's passage, the Colorado Privacy Act (CoPA) became law in July 2021 and the Connecticut Personal Data Privacy and Online Monitoring Act (CTDPA) became law in May 2022. Both statutes define Dark Patterns in materially identical terms⁴³ to the CPRA and both similarly nullify a consent if it was obtained by use of a Dark Pattern.⁴⁴ When the CPRA, CoPA and CTDPA—and their respective UX-regulating provisions—each come into effect during 2023,⁴⁵ they will formally usher the proscription and regulation of Dark Patterns, by name, into the online user experience.

Although these state statutory schemes will only protect their respective residents and apply to certain entities, thanks to California's standing as the world's fifth largest economy⁴⁶ and the global reach of many of the companies the statutes will collectively impact; adhering to their terms must be a significant priority not only to avoid short-term financial penalties,⁴⁷ but also to advance long-term business strategies and growth.

Despite the rapidly approaching 2023 effective dates for the California, Colorado and Connecticut data privacy laws and the mass of draft data privacy bills currently undergoing varying degrees of starts and fits in state legislative houses throughout the country,⁴⁸ state law enforcement bodies have not been waiting idly by for manipulative design-specific laws to emerge. Instead, numerous chief law enforcement officers have chosen to rely upon their respective state's existing consumer protection laws to bring actions to curb the tide of Dark Pattern practices.

In January 2022, the Attorneys General for the District of Columbia and the states of Washington, Texas and Indiana

filed coordinated lawsuits against Google alleging the tech giant's rapacious use of Dark Patterns to, e.g., unlawfully manipulate and outright deceive their resident-consumers to obtain desired location and tracking data.⁴⁹ Each lawsuit was brought under each state's and the District's respective existing consumer protection statutes.⁵⁰

In March 2022, the New York Attorney General relied on her broad statutory authority to prohibit deceptive acts and practice in reaching a \$2.6 million settlement with a hybrid online travel agency⁵¹ for using entirely fabricated messaging prompts to create a false sense of scarcity and urgency during the ticket purchasing process as to the quantity of tickets remaining and the population of similarly interested buyers, e.g. "Book Now: Only X tickets left," and "X other people are looking at this flight," as well as generating unsupported figures at the purchase screen to nudge the completion of a purchase, e.g. "X people protected their trip by purchasing travel insurance."⁵²

Not surprisingly, governmental authorities are not alone in taking aim at the rise of Dark Patterns. The class action plaintiff's bar has gotten in on the act with a very notable recent success. In February 2022, a \$62 million settlement was reached against Noom to resolve a putative class action alleging that the subscription-based weight loss app used a variety of Dark Patterns—including trick wording, visual interference and Roach Motel-subscription methods—against its subscribers.⁵³ The pleadings alleged violation of 59 distinct consumer protection statutes from all 50 states, the District of Columbia and three territories.⁵⁴

This fight against Dark Patterns, much like the digital economy itself, is not however, confined to our shores. Although the European Union's privacy law known as the GDPR⁵⁵ does not explicitly prohibit Dark Patterns, earlier this year France's data protection regula-

tor applied the European Union's ePrivacy Directive⁵⁶-based authority to fine Google €150 million and Facebook/Meta €60 million apiece for their respective designs architectures which effectively required users to perform several clicks to refuse cookies but only a single click to accept them.⁵⁷ The European Data Protection Board—established by the GDPR specifically to promote the consistent application of data protection rights throughout the European Union—recently published guidelines on how to recognize and combat Dark Patterns in social media platforms⁵⁸ and the wide-ranging Digital Services Act,⁵⁹ which will largely ban the use of Dark Patterns throughout the European Union, was adopted by the European Parliament in July 2022 with a likely effective date in early 2024.⁶⁰

How to Root Out and Prevent

The wave of enforcement and litigation-based actions aimed at beating back the pervasive use of Dark Patterns has only just begun to crest, so how best can we help navigate clients—and their interfaces—among the often-imprecise borders between a persuasive design and an unlawful Dark Pattern? In addition to the vital—and perpetual—task of keeping abreast of the rapidly changing domestic and foreign regulatory landscapes on this front, the following are some suggestions:

First, do not become complacent simply because most actions have thus far been directed mainly at the shiniest online presences and most egregious practices. Regardless of a client's current size, scope, location or existing user demographics, take a 10,000-foot view of its interfaces and functionalities through the lens of the Fair Information Practice Principles (FIPPs).⁶¹ Of special importance when examining the overall design construction and Choice Architecture features will likely be the Openness Principle, i.e. is there consistent transparency

with the user about *who* may be collecting data and *why* it would be collected?, the Individual Participation Principle, i.e. is the user *clearly* being presented that ability to easily obtain information from the data controller?, and the Accountability Principle, i.e. are there compliance structures in place to *ensure and verify* that the intended design functionalities perform properly?

Next, narrow your gaze to objectively analyze if the design construction, resulting rendered environment and operational practices themselves—either individually or collectively—could reasonably be seen as deceptive or unfair to any degree. Ask, does the UX *feel* like it puts the user at a disadvantage either in terms of the form of information being provided or in the fairness of how such information is presented? When undertaking this analysis, be sure to drill down on the *outcome* of the design and not the design's intent. The CPRA and its Colorado and Connecticut privacy law cousins all share that type of result-directed emphasis and they may well serve as models for future design-directed privacy schemes to come.

Finally, be sure to inform your perpetual evaluations by closely and regularly collaborating with operations and architectural client-side folks. This type of teamwork will not only provide you with a richer appreciation of the client's unvarnished strategies and internal functionalities throughout the developmental, launch, and operational stages of any product or presence but it will afford you the openings needed to introduce and instill some anti-Dark Patterns best practices deep within the creative pipeline. As with most digital endeavors that can rapidly evolve and develop, often sunlight and inquisitive curiosity will serve as trusty guideposts to keep online practices on the straight and narrow. ■

Endnotes

1. Scholarship has explored this practice of methodically commandeering the will of a user by altering the surroundings and context within which online visitors make decisions, a concept known as "choice architectures." See, e.g., Richard H. Thaler, Cass R. Sunstein & John P. Balz, *Choice Architecture*, The Behavioral Foundations of Public Policy 428, 428 (Eldar Shafir ed., 2013).
2. See Jennifer King & Adriana Stephan, *Regulating Privacy Dark Patterns in Practice - Drawing Inspiration From California Privacy Rights Act*, 5 Geo. L. Tech Rev. 250, 251 (2021)
3. Harry Brignull, Ph.D, is a United Kingdom-based user experience expert who first used the term "Dark Patterns" to describe a purposefully manipulative user interface design. He has operated the website *darkpatterns.org* since 2010 as a clearing house for the examination and posting of perceived Dark Patterns and other questionable user experience and user interface practices.
4. A design pattern is a "reusable/recurring component[] which designers use to solve common problems in user interface design." See interaction-design.org/literature/topics/ui-design-patterns. Dr. Brignall has explained that the term Dark Pattern is based on the concept of a design pattern and that "when purposeful deception impacts the design pattern, a dark pattern results." Statement of Harry Brignall, Ph.D. on April 29, 2021. (ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf)
5. The term Dark Patterns is "meant to communicate the unscrupulous nature and also that fact it can be shadowy and hard to pin down." Statement of Harry Brignall, Ph.D. on April 29, 2021. (ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf)
6. *Jacobellis v. Ohio*, 378 U.S. 184, 197 (1964) (Stewart, J., concurring) (In discussing the presence of hard-core pornography, famously stating "[b]ut I know it when I see it, and the motion picture involved in this case is not that.")
7. See e.g., deceptive.design/types
8. See Thaler, et al., *supra* at note 1.
9. Arunesh Mathur, et al. 2021. What Makes a Dark Pattern...Dark?: Design Attributes, Normative Considerations, and Measurement Methods. In *CHI Conference on Human Factors in Computing Systems* (CHI ,21), May 8-13, 2021, Yokohama, Japan. ACM, New York, NY, USA. 27 pages. [doing.org/10.1145/3411764.3445610](https://doi.org/10.1145/3411764.3445610)
10. deceptive.design/types
11. *Id.*
12. *Id.* This category, colloquially termed a *Basket Sneak* is materially similar to a Negative Option feature which is defined by the Federal Trade Commission's Telemarketing Sales Rule as "a provision in an offer or agreement to sell or provide any good or services 'under which the customer's silence or failure to take an affirmative action to reject goods or services or to cancel the agreement is interpreted by the seller as acceptance of the offer.'" 16 C.F.R. § 310.2(w).
13. deceptive.design/types
14. *Id.*
15. *Id.* This term is a call back to the popular Black Flag® pest control device television commercials of the late 1970s and early '80s where,

thanks to the deadly one-way design of the traps, the tagline was roaches would “check in but they don’t check out.” See, e.g., [youtube.com/watch?v=z4c2gadmytg](https://www.youtube.com/watch?v=z4c2gadmytg)

16. *deceptive.design/types*

17. *Ibid.*

18. *Ibid.*

19. *Ibid.*

20. *Ibid.*

21. *Ibid.*

22. Colin M. Gray, et al. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) (CHI’18). AMC, New York, NY, USA Article 534, 14 pages. doi.org/10.1145/3173574.3174108

23. *Id.*

24. *Id.*

25. *Id.*

26. See, e.g., Mathur, et al., *supra* at note 9.

27. This wide gamut is monitored by two major virtual tip line websites, one maintained by Dr. Brignall at *deceptive.design/hall-of-shame/all* and the other by the Stanford University’s Digital Civil Society Laboratory at *darkpatternstipline.org*

28. Although the Privacy Act of 1974 governs the collection and use of certain information about individuals maintained by federal agencies, it does not regulate non-federal entities to any degree. See 5 U.S.C. § 552a, et seq. However, numerous federal bills continue to be introduced to address overall private sector privacy protection concerns. The most significant recent example is the Deceptive Experiences To Online Users Reduction Act (DETOUR Act) which was reintroduced in December 2021 by a bipartisan group of U.S. Senators and, in its current proposed form, would prohibit large online operators from designing, modifying

or manipulating a user interface “with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data,” however; at press time the bill remains in Committee. See [congress.gov/117/bills/s3330/BILLS-117s3330is.pdf](https://www.congress.gov/117/bills/s3330/BILLS-117s3330is.pdf)

29. See, e.g., FTC v. Prog Leasing, LLC, Civil Action No. 1:20-mi-00000-UNA (detailing a \$175 million settlement with a company that markets rent-to-own payments plans for tens of thousands of retail stores nationwide for its failure to obtain express, informed consent to consumer charges, in violation of Section 5 of the FTC Act); FTC v. Age of Learning, LLC, Civil Action No. 2:20-cv-7996 (detailing a \$10 million settlement with the online children’s education company for, e.g., improperly using negative option marketing, in violation of Sections 13(b) and 19 of the FTC Act and the Restore Online Shoppers’ Confidence Act).

30. See [ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop](https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop)

31. See Enforcement Policy Statement Regarding Negative Option Marketing ([ftc.gov/system/files/documents/public_statements/1598063/negative_option_policy_statement-10-22-2021-tobureau.pdf](https://www.ftc.gov/system/files/documents/public_statements/1598063/negative_option_policy_statement-10-22-2021-tobureau.pdf))

32. gizmodo.com/ftc-probing-deceptive-amazon-prime-signup-tricks-18486546109.

33. This investigation may have been foreshadowed, or even bolstered, by the work of EPIC, a powerful privacy advocacy group that filed a formal complaint with the Office of the Attorney General for the District of Columbia in February 2021 alleging Amazon’s use of Dark Patterns in purported violation of both the

District of Columbia’s Consumer Protection Procedures Act and the Federal Trade Commission Act. See epic.org/wp-content/uploads/privacy/dccppa/amazon/EPIC-Complaint-In-Re-Amazon.pdf

34. See Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (2018).

35. It has been contended that such an exercise of existing Section 5 powers alone affords the FTC the ability to sufficiently reign in Dark Patterns in the marketplace and beyond. See epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDDataMinimization_012522_VF_.pdf

36. California has a proud history of legislating to protect its resident’s privacy rights. For example, in 2004 it passed the California Online Privacy Protection Act (CalOPPA) which was the first in the nation law to require website operators to post privacy policies setting forth their information handling practices. See Cal. Bus. & Prof. Code §§ 22575-22579.

37. California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.198(a) (2018).

38. California Consumer Privacy Act, Cal. Civ. CODE REGS. tit. 11, § 999.315(h) (2021).

39. California Privacy Rights Act, Cal. Civ. CODE § 1798.100 et seq. (eff. Jan 1, 2023).

40. California Privacy Rights Act, Cal. Civ. CODE § 1798.140(l) (eff. Jan. 1, 2023).

41. *Id.* at § 1798.140(h) (2021).

42. The CPRA created the nascent California Privacy Protection Agency (CPPA) which is charged with implementing and enforcing new privacy rules. See California Privacy Rights Act, Cal. Civ. CODE § 1798.199.40(a). The CPPA’s Executive Director Ashkan Soltani

- has officially stated that formal rulemaking applicable to the CPRA will be completed in “Q3 or Q4” of 2022. *See* iapp.org/news/a/cpra-regulations-delayed-past-july-1-deadline-expected-q3-or-q4/
43. Although the substantive definitions are the same, the CoPA does not include the CPRA’s trailing qualifier: “as further defined by regulation,” *see* C.R.S. 6-1-1303(9) and the CTDPA specifically includes “any practice the Federal Trade Commission refers to as a ‘dark pattern.’” *See* cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF at *Sec.* 1(11)(B)
 44. *See* C.R.S. 6-1-1303(9); C.R.S. 6-1-1303(5)(c) and cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF at *Sec.* 1(6)(C)
 45. The CPRA will become effective on Jan. 1, 2023, and the CoPA and CTDPA will both become effective on July 1, 2023.
 46. *See* bea.gov/
 47. Under the CPRA, in addition to injunctive relief, administrative fine or civil penalties between \$2,500 and \$7,500 can be levied per violation. *See* Cal. Civ. CODE §§1798.155(a); 1798.199.90(a). Under the CoPA, a violation is deemed a deceptive trade practice under the Colorado Consumer Protection Act so, in addition to injunctive relief, a penalty of up to \$20,000 per violation could be assessed. *See* C.R.S.A. § 6-1-1311(1)(c). Under the CTDPA, a violation is deemed an unfair trade practice under the Connecticut Unfair Trade Practices Act so, in addition to injunctive relief, a penalty of up to \$25,000 per violation could be assessed. *See* C.G.S.A. § 42-110o.
 48. International Association of Privacy Professionals, *US State Privacy Legislation Tracker*, iapp.org/resources/article/us-state-privacy-legislation-tracker/ (April 1, 2021). As for New Jersey’s efforts to join the state privacy law movement, the New Jersey Disclosure and Accountability Transparency Act (NJ DaTA) was reintroduced as Assembly Bill No. 505 in January 2022 but at press time, it remains in Committee without any indication of movement this session. Nevertheless, the proposed NJ DaTA, in its current form, does not contain any Dark Pattern proscriptions.
 49. *See* (District of Columbia’s Complaint) oag.dc.gov/sites/default/files/2022-01/DCv.Google%281-24-22%29.pdf; (Washington’s Complaint) agportals3bucket.s3.amazonaws.com/uploadedfiles/Another/News/Press_Releases/2022_01_24FinalRedactedComplaint.pdf; (Texas’s Complaint) texasattorneygeneral.gov/sites/default/files/image/s/executive-management/Google%20Geolocation%20Original%20Petition-fm.pdf; (Indiana’s Complaint) content.govdelivery.com/attachments/INAG/2022/01/24/file_attachments/2055802/Google%20-%20Complaint%20-%20PUBLIC%20Redacted.pdf
 50. *Id.*
 51. *See* ag.ny.gov/sites/default/files/2022.03.16_nyag-fareportal_aod_fully_executed.pdf
 52. *Id.*
 53. *See* reuters.com/legal/litigation/noom-diet-app-reaches-62-mln-settlement-over-automatic-subscription-renewals-2022-02-14/
 54. *See* Nichols, et al. v. Noom, Inc., et al, Third Amended Complaint (Doc. No. 174) Civil Action No. 1:20-cv-3677-KHP (SDNY).
 55. The General Data Protection Regulation became effective on May 25, 2018, throughout all European Union member states and provides European customers with numerous data privacy rights including rights to know, to access, to object, to restrict processing and to portability. *See generally*, General Data Protection Regulation, Ch.3, gdpr-info.eu/chapter-3/
 56. The Privacy and Electronic Communications Directive 2002/58/EC, commonly known as the ePrivacy Directive, addresses cookie usage, data minimization and other related data privacy aspects in the European Union.
 57. *See* legifrance.gouv.fr/cnil/id/CNILTEXT000044840062; legifrance.gouv.fr/cnil/id/CNILTEXT000044840532
 58. *See* edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf
 59. *See* europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.html
 60. *See* europarl.europa.eu/news/en/press-room/20220701IPR34364/digital-services-landmark-rules-adopted-for-a-safer-open-online-environment
 61. Developed in 1980 by the international Organization for Economic Cooperation and Development, the FIPPs were later codified in the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and has since become the recognized standard by which to measure privacy measures. iapp.org/resources/article/fair-information-practices/



Legal Malpractice Insurance Premiums Are Shocking New Jersey Law Firms

We can help! Just ask any of the over 1400 New Jersey law firms who already entrust us with their legal malpractice coverage.

Garden State Professional Insurance Agency is the exclusive agent in NJ for the largest legal malpractice insurer in the country and we represent many other insurers rated *Superior & Excellent*. We also have good homes for firms with less-than-perfect claim records or difficult areas of practice.

Looking for other coverages for your firm? We provide Cyber Liability and Employment Practices coverage also!

Contact us for a no obligation consultation and premium estimate.

800-548-1063
info@gsagency.com
www.gsatency.com



NJSBA

2022
Mid-Year Meeting

KEY WEST

November 6-10
Casa Marina Key West

REGISTER TODAY
NJSBA.COM

