



The State Bar of California

II.I. Confid. & Data Secur.
08-11-21 CTJG Meeting
Open Session

CLOSING THE JUSTICE GAP WORKING GROUP

Date: July 7, 2021

To: Scope Subcommittee

From: David Freeman Engstrom and Kevin Mohr

Subject: II.I. Client Confidentiality, Data Security, and the Attorney-Client Privilege in a Proposed Sandbox

INTRODUCTION

This memo provides a brief overview of some issues relating to client confidentiality, data security, and the attorney-client privilege in a proposed sandbox. It has four parts. First, we briefly treat what types of data and information are likely to be of most concern. Next, we focus in on what we see as a principal design challenge: how to deal with already-existing rules and regulations governing confidentiality and data privacy and security, which raise the possibility that different sandbox entrants might be subject to rules of varying stringency. Third, we consider the special case of the attorney-client privilege and show why it may prove less important than the broader duty of confidentiality. Finally, we offer some concrete approaches the working group might consider in an ultimate sandbox recommendation, distinguishing between rules covering voluntary disclosure (*i.e.*, commercialization), involuntary disclosure (*i.e.*, hacks), and compelled disclosure (*i.e.*, legal proceedings). These are not comprehensively framed proposals but rather an attempt to spur concrete discussion at our next meeting.

WHAT DATA SHOULD WE BE WORRIED ABOUT?

A preliminary question is what types of data would be sufficiently valuable that such data could plausibly be commercialized by a sandbox entrant or, alternatively, could plausibly be the target of a hack or data breach. A useful look at that question can be found in a 2015 law review article providing a “sensitive information taxonomy” of roughly a dozen types of data that can

be gleaned from court records.¹ Two strike us as plausible illustrations of potentially commercially valuable data in the sandbox context: (i) financial, health, demographic, and familial information that can be used by companies, particularly data brokers, to target advertising to potential consumers (*e.g.*, divorce records for purposes of marketing fitness services to newly single women²); and (ii) past involvement in civil or criminal proceedings with commercial implications (*e.g.*, prior landlord-tenant proceedings, which landlords might use to construct blacklists of tenants,³ prior bankruptcy proceedings, which might help secured-credit-card companies to identify customers). This by no means exhausts the possibilities. As the law review article notes, litigation is a place where life's dramas are performed. The same could prove true of a sandbox.

THE CHALLENGE OF ALREADY-EXISTING ETHICS RULES AND REGULATIONS

A key challenge, in our view, will be how to contend with existing regulatory schemes that might bind some but not all sandbox entrants, making it possible that entrants will be subject to rules of varying stringency. For example:

- Under rule 1.6 of the California Rules of Professional Conduct, lawyers have a duty of confidentiality.⁴ With only a few exceptions, the release of any client information, not just client secrets, can subject a lawyer to liability and misconduct proceedings. This is true even with involuntary information releases or releases that result from malicious acts by third-parties. Importantly, the duty of confidentiality has been interpreted to include a duty to employ reasonably available technical means to prevent cyber theft and data leaks, regardless of whether performed in-house or by a vendor or the

¹ David S. Ardia & Anne Klinefelter, *Privacy and Court Records: An Empirical Study*, 30 Berkeley Tech L.J. 1807 (2015), available at https://scholarship.law.unc.edu/faculty_publications/15/.

² Karen Gottlieb, *Using Court Record Information for Marketing in the United States: It's Public Information, What's the Problem?*, Privacy Rights Clearinghouse (Feb. 1, 2004), <https://privacyrights.org/resources/using-court-record-information-marketing-united-states-its-public-information-whats>.

³ Kim Barker & Jessica Silver-Greenberg, *On Tenant Blacklist, Errors and Renters with Little Recourse*, N.Y. TIMES (Aug. 16, 2016), <https://www.nytimes.com/2016/08/17/nyregion/new-york-housing-tenant-blacklist.html>; Rhonda Kaysen, *How to Escape the Dreaded 'Tenant Blacklist'*, N.Y. TIMES (Apr. 13, 2019), <https://www.nytimes.com/2019/04/13/realestate/how-to-escape-the-dreaded-tenant-blacklist.html>.

⁴ Rule 1.6(a) provides: "A lawyer shall not reveal information protected from disclosure by Business and Professions Code section 6068, subdivision (e)(1) unless the client gives informed consent, or the disclosure is permitted by paragraph (b) of this rule." In turn, section 6068(e)(1) provides that it is a duty of a lawyer: "To maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client."

technique (*e.g.*, cloud computing).⁵ Related to rule 1.6 in this regard is the duty of competence under rule 1.1(b)'s requirement that a lawyer "apply the (i) learning and skill, and (ii) mental, emotional, and physical ability reasonably necessary for the performance of such service." This includes a duty to keep abreast of changes in law and technology, a duty of competent use of technology to transmit or store confidential client information, and a duty of competence following a data breach. Finally, rule 1.9 prohibits use of information from a past representation in aid of a present client in a way that works to the disadvantage of the past client. All three rules would apply in full to a licensed lawyer operating within the sandbox. This creates a potential asymmetry within the sandbox: Barring the adoption of specific rules that would apply to all sandbox participants, lawyer entrants might be subject to more stringent constraints than non-lawyer entrants.

- The California Consumer Privacy Act (as amended by its Proposition 24 successor, the California Privacy Rights Act) is another already-existing regulatory scheme that would likely bind some but not all sandbox entrants. The CCPA grants a full set of rights to data subjects: a right to notice that their data is being collected and used and the right to opt out, access their own data, and correct or delete that data. However, the CCPA covers only large-ish entities satisfying one of the following: (i) > \$25 million in annual revenues; (ii) data holdings on at least 50,000 Californians or households; (iii) deriving more than half of revenue from data sales. That means that the CCPA might apply to some sandbox entrants (*e.g.*, a RocketLawyer-scale provider) but not others.
- Non-lawyer providers who aren't subject to the CCPA will instead be regulated by a residuum of data security and privacy laws and regulations: sectoral regulations (*e.g.*, HIPAA for health care, various data privacy rules governing banking); consumer protection laws (*e.g.*, FTC Act Sec. 5, CA's UDAP); and breach notification statutes (*e.g.*, CAL. CIV. CODE § 1798.82).

What to do? The easiest, lowest-friction option would be to level up and make compliance with all existing duties under rules 1.6/1.1/1.9 and the CCPA a contractual condition of sandbox entry. Incorporating these rules in full would presumably also mean incorporating any changes to those rules, or changes in their interpretation, that may occur over time, ensuring that the rules will evolve along with technological developments rather than remaining static and becoming outmoded.

There are, on the other hand, reasons not to do this. First, we might determine that asymmetries are justified and even wise. For instance, the CCPA applies to large entities because those entities are capable of greater consumer harm and because those entities enjoy economies of scale and so are more capable of taking sophisticated precautions. The fixed cost

⁵ For a good summary, see <http://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/2010-179-Interim-No-08-0002-PAW.pdf>.

of compliance—legal advice, technical infrastructure—may have a regressive effect for smaller and less sophisticated sandbox entrants. This may be particularly the case with the CCPA’s more onerous data subject and cybersecurity requirements.

Second, there may be legal services delivery models that depend on limited disclosure of information. One example, to our mind, is a tech-based provider who aggregates client data to refine or tailor services provided to future customers/clients. Thus, a firm like RocketLawyer might use its repository of past representations to optimize service delivery in future ones. We were not able, with the time we had, to find any case law or regulatory schemes that cover this situation. On the one hand, disclosure to fellow members of a law firm is impliedly authorized by the establishment of an attorney-client relationship.⁶ It follows that representations become part of the collective intelligence of the firm that can be used in further representations. On the other hand, the duty of confidentiality precludes a lawyer from making disclosures that do not directly reveal protected client information but could reasonably lead to third-party discovery of that information.⁷ For instance, a tech-based provider’s provision of services to present clients that are known to be based on data drawn from past representations could conceivably permit a sophisticated third party to infer something about the identity of a past customer/client or the particular services that were provided to that customer/client. A second example is that sandbox entrants might propose a business model that involves some limited commercialization of customer/client data in order to generate revenue that can subsidize the provision of legal services. Indeed, the viability of a model that serves lower-income individuals might depend on commercialization. Customers/clients and their data would, Facebook-like, become part of the product. Both of these possibilities require further research. Group brainstorming about other examples might also be useful, as would input from Crispin Passmore or others about the U.K. experience with commercialization.

Perhaps the most pro-innovation way to contend with already-existing rules and regulations would be to level down across the board and subject all entrants, whether lawyers or not and whether subject to the CCPA or not, to relaxed versions of each. For instance, given that a sandbox is likely to require legislative authorization in any event, one could imagine a sandbox that switches off some or all of the requirements of rules 1.6/1.1/1.9 and the CCPA. This would make the sandbox at least in part an experiment in legal-services-related confidentiality and data security. That said, given California’s traditionally strong protection of client confidentiality, relaxation of the duty would likely present a steep hurdle.

⁶ ABA Model Rule 1.6, Comment [5]; San Diego Bar Ass’n Form.Opn. 1996-1; ABA Form.Opn. 08-453 (implied authorization includes consulting in-firm “ethics counsel” re ethical implications of consulting lawyer’s conduct).

⁷ ABA Model Rule 1.6, Comment [4]; see Los Angeles County Bar Ass’n Form.Opn. 529 (2017) (discussing possibility that opposing party or third person might infer client’s identity from context of disclosure on social media).

THE ATTORNEY-CLIENT PRIVILEGE

Compared to the duty of confidentiality, the attorney-client privilege might at first glance appear to be of less concern to the design of a sandbox. The attorney-client privilege is powerful but narrow: It applies only to confidential communications between a client and an attorney or agent made for the purpose of seeking legal advice. It comes into play primarily in court proceedings, protecting client-lawyer communications from being admitted in evidence against the client. The duty of confidentiality, a kind of duty not to gossip about one's client, covers far more information, whether or not communicated by the client. It will be the primary constraint on commercialization and also the primary source of cybersecurity obligations.

Nevertheless, the attorney-client privilege will be implicated for sandbox entrants when a third party seeks, as part of a legal proceeding, to compel a sandbox entrant or its customer/client to disclose covered communications. The privilege is critical in providing the client with assurance that communications between lawyer and client that might result in disclosure of information embarrassing or detrimental to the client are protected from disclosure. This provides the client with an incentive to disclose information the lawyer needs to competently and effectively represent the client. Consequently, it makes sense to provide for it in our proposal. As with the duty of confidentiality and the CCPA, a key question will be whether to adopt a consistent approach across all entrants—for instance, by attaching the attorney-client privilege in full to non-lawyer sandbox entrants—or tolerate a mixed approach where the services provided by some entrants (by virtue of being lawyers) will be subject to the benefits and obligations of the privilege but not others.

Note that applying the attorney-client privilege to nonlawyers would not be novel: Many jurisdictions now have confidentiality that covers nonlawyers who do mediation. In addition, there is now recognized to be a privilege between nonlawyers who are authorized to practice before the U.S. Patent and Trade Office and patent clients. Further research might surface other examples—for instance, Washington state's LLLT program, Arizona's recent reforms, which determined that ABSs were practicing law, or the United Kingdom. We might also engage with the California Paraprofessional Program Working Group for their thinking on the issue.

Remaining concerns here are mostly academic, at least for the moment: Could (or even should) AI agents be covered by the attorney-client privilege?⁸

⁸ Michael Stockdale & Rebecca Mitchell, *Legal Advice Privilege and Artificial Legal Intelligence: Can Robots Give Privileged Legal Advice?*, 23 INT'L J. OF EVID. & PROOF 422 (2019).

POSSIBLE APPROACHES

When thinking about possible approaches, it may be useful to think separately about options for regulating voluntary data disclosures (*i.e.*, commercialization), involuntary data disclosures (*i.e.*, hacks), and compelled disclosures (*i.e.*, in a legal proceeding). Our ultimate proposal could then mix and match individual options from the three categories.

For voluntary disclosure (*i.e.*, commercialization), there are four possibilities:

- flatly prohibit commercialization of any kind as a condition of entrance
- incorporate by reference rules 1.1/1.6/1.9 and the CCPA for all entrants (leveling up), which would likely have the same effect of prohibiting commercialization.
- permit limited commercialization with justification, but rules 1.1/1.6 and the CCPA continue to apply to eligible entrants (a mixed approach)
- permit limited commercialization with justification for all entrants, thus limiting the application of rules 1.1/1.6/1.9 and the CCPA across the board (leveling down)

For involuntary disclosure (*i.e.*, data security and hacks), there are three possibilities:

- incorporate by reference rules 1.1/1.6/1.9 and the CCPA for all entrants (leveling up)
- condition entrance on evidence of “reasonable” precautions to safeguard customer/client data, but rules 1.1/1.6/1.9 and the CCPA continue to apply to eligible entrants (a mixed approach)
- condition entrance on evidence of “reasonable” precautions to safeguard data for all entrants, thus pausing rules 1.1/1.6/1.9 and the CCPA across the board (leveling down)

For instances of compelled disclosure as part of a legal proceeding, there are two possibilities⁹:

- apply the attorney-client privilege in full to sandbox entrants (leveling up)
- do not apply the attorney-client privilege to sandbox entrants, but it will continue to apply to law

⁹ There are only two options here because leveling down, and switching off the privilege even for sandbox entrants who are lawyers, strikes as a bad idea and different in kind from relaxing the duty of confidentiality or CCPA to facilitate limited commercialization of client data or reduce regulatory burdens.