UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF VERMONT

JANET JENKINS, et al., Plaintiffs, v. KENNETH L. MILLER, et al., Defendants.	No. 2:12-cv-184-WKS

PLAINTIFFS' REPLY IN SUPPORT OF THEIR MOTION TO COMPEL DEFENDANTS LIBERTY COUNSEL, INC. AND RENA LINDEVALDSEN TO COMPLY WITH PLAINTIFFS' REQUESTS FOR PRODUCTION

Plaintiff Janet Jenkins filed this action to hold accountable those involved in the September 2009 international kidnapping of her then-seven-year-old daughter Isabella Miller-Jenkins, who remains missing a decade later, simply because Jenkins is a lesbian. Three individuals have been convicted for their involvement in that crime, and this Court has since held that Plaintiffs sufficiently allege Defendants Liberty Counsel, Inc. and Rena Lindevaldsen were also involved in the conspiracy to kidnap Isabella. As is their right under the Federal Rules of Civil Procedure, Plaintiffs seek to discover relevant evidence from Defendants.

Tellingly, much of Defendants' response in opposition, ECF 374 ("Resp."), to Plaintiffs' motion to compel, ECF 361 ("Mot. to Compel"), is devoted not to the merits of Plaintiffs' discovery requests ("Requests") but rather to the alleged, untrue, and (in any event) irrelevant motivations of some of Plaintiffs' attorneys for representing Plaintiffs in this lawsuit. Defendants' belief that this case is no more than an attempt by certain lawyers representing Jenkins to "destroy" them does not excuse them from the discovery process. The motion to compel should be granted.

I. Plaintiffs' Well-Pleaded Claims Justify the Requests.

The Requests seek evidence to support Plaintiffs' well-pleaded claims that Defendants violated Plaintiffs' civil and parental rights. Rule 26 of the Federal Rules of Civil Procedure permits Plaintiffs to seek discovery regarding "any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case." *Connolly v. Alderman*, No. 2:17-cv-79, 2018 WL 4462368, at *5 (D. Vt. Sept. 18, 2018) (Reiss, J.) (quoting *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978)).

A. The Complaint's Allegations Support the Requests.

The facts alleged in the Revised Second Amended Complaint, ECF 223 ("Compl."), are sufficient to justify the Requests. The requirement that discovery requests be justified by a "*modicum* of objective support" does not narrow the broad scope of Rule 26, but merely serves to ensure that requests are not "based on pure speculation or conjecture." *Tottenham v. Trans World Gaming Corp.*, No. 00-Civ.-7697, 2002 WL 1967023, at *2 (S.D.N.Y. June 21, 2002) (emphasis added). Moreover, allegations in the pleadings may provide the modicum of objective support necessary to justify discovery requests. *See id.* (pointing to specific allegations in defendants' answer to justify requests regarding counterclaim).

Requests 4 through 8 seek all documents and communications concerning Jenkins, Isabella, and Defendant Lisa Miller, as well as all communications with Isabella and Lisa Miller. These Requests are supported by allegations demonstrating that much of Defendants' involvement in the lives of Jenkins, Isabella, and Lisa Miller has been motivated by Defendants' desire to keep Isabella away from Jenkins. Specifically, Plaintiffs allege that Defendants sought out Lisa Miller in 2004 to assist in her custody battle against Jenkins, Compl. ¶ 21, ECF 223, and that Defendants encouraged Lisa Miller to move with Isabella to the Lynchburg, Virginia area—

where Defendants were located—in early 2008. *Id.* ¶ 24. It was during this time period, while Lisa Miller and Isabella were living near Defendants and attending church with Lindevaldsen, that Lisa Miller stopped permitting visitation between Isabella and Jenkins after a brief period of compliance. *Id.* ¶¶ 23–24. Shortly thereafter, in or about June 2008, the conspiracy to kidnap Isabella was hatched. *Id.* ¶ 25. Around the same time, Defendants began contracting with Defendant Response Unlimited, Inc., which was owned by Defendant Philip Zodhiates—the co-conspirator who would eventually drive Lisa Miller and Isabella to the Canadian border. *Id.* ¶ 29. The kidnapping was the "personal option" that Zodhiates offered to Defendants in early 2009. *Id.* Following the kidnapping, Lindevaldsen continued to communicate indirectly with Lisa Miller, *id.* ¶ 44, and facilitated the removal of items from Lisa Miller's home. *Id.* ¶ 45.

Request 8, which asks for "all communications with Lisa Miller," is further supported by allegations that Defendants specifically communicated with Lisa Miller about the conspiracy to kidnap Isabella. Plaintiffs allege that Liberty Counsel told Lisa Miller that "it would be in her best interests to disappear," *id.* ¶ 41, that Zodhiates and Defendant Victoria Hyden facilitated communications between Lisa Miller and Lindevaldsen after the kidnapping, *id.* ¶ 46, and that Lisa Miller entrusted her diaries to Lindevaldsen before her disappearance. *Id.* ¶ 62.

Requests 11 and 12 seek communications with two of Lisa Miller's known email addresses, respectively, regarding specific subjects, and are justified by the same facts as Requests 4 through 8.

Request 17 seeks "all documents and communications concerning the Dispute." This Request is supported by the allegations that Defendants have been involved in the Dispute since 2004, *id.* ¶ 21, and that, between 2004 and summer 2009, Defendants' representation of Lisa Miller in the Dispute crossed the line into conspiracy to kidnap Isabella. *Id.* ¶ 34. Plaintiffs

further allege that certain actions taken by Defendants as part of the Dispute were done in furtherance of the conspiracy, including Lindevaldsen's misrepresentation to the Rutland Family Court concerning Lisa Miller's whereabouts in December 2009. *Id.* ¶¶ 49–50; *see also id.* ¶ 61. Lindevaldsen wrote a book about the Dispute, which she and Liberty Counsel President Mathew Staver promoted on radio and television. *Id.* ¶ 62.

Request 18 seeks "all documents and communications concerning the Court Orders."[1] This Request is supported by the allegation that Defendants assisted and encouraged Lisa Miller to flout the Court Orders beginning in 2004, *id.* ¶ 20, as well as by the allegation that Lisa Miller resumed her contempt of the Court Orders after a brief period of compliance when she moved to be near Defendants in early 2008. *Id.* ¶¶ 23–24. This Request is further supported by the allegations regarding Defendants' own actions in furtherance of the conspiracy to flout the Court Orders, including their misrepresentations to the courts of Vermont and Virginia.[2] *Id.* ¶ 61.

Request 19 seeks all communications on November 20, 2009, which is supported by the allegation that this was the date on which the Rutland Family Court transferred custody of Isabella to Jenkins. *Id.* ¶ 47.

Request 35 seeks all communications on September 20–22, 2009, while Request 36 seeks information regarding events that happened or were planned to happen on those dates. These

[1] "Court Orders" means "any order issued or expected to be issued by a state court of Vermont or Virginia concerning Plaintiff Isabella Miller-Jenkins, including but not limited to any order issued in the Vermont Proceedings, including but not limited to the Custody Transfer Order, or in the Virginia Proceedings." *E.g.*, Pls.' First Set of Reqs. for Produc. to Def. Rena Lindevaldsen at *3, ECF 361-1; *see also id.* (defining "Custody Transfer Order"); *id.* at *5 (defining "Vermont Proceedings" and "Virginia Proceedings").

[2] Lindevaldsen and Staver also co-taught a course at Liberty University School of Law for which students were given an exam question asking them to place themselves in Lindevaldsen's and Staver's shoes in advising Lisa Miller on whether to comply with the Court Orders. *See* Op. & Order at 45–46, ECF 220.

Requests are supported by the allegation that Lisa Miller and Isabella were picked up from a Walmart parking lot on September 20, 2009, *id.* ¶ 44, and that Isabella was kidnapped on September 21, 2009, *id.* ¶ 36. They are further supported by the allegation that Zodhiates made phone calls to phone numbers registered to Liberty Counsel and Liberty University, where Liberty Counsel had an office, on September 22, 2009, between 1:28 and 1:30 p.m., while he was en route back to Virginia from depositing Lisa Miller and Isabella at the Canadian border. *Id.* ¶ 60.

Request 47 seeks all communications on November 9–13, 2009, while Request 48 seeks information regarding events that happened or were planned to happen on those dates. These Requests are supported by the allegation that Lindevaldsen facilitated the removal of belongings from Lisa Miller's home during this time period. *Id.* ¶ 45.

These facts provide well more than the modicum of objective support sufficient to justify Plaintiffs' Requests to obtain information related to their conspiracy allegations. *See Tottenham*, 2002 WL 1967023, at *2. Defendants' demand for more, *see* Resp. at 6, ECF 374, misunderstands the difference between claims that involve "discrete and discernible physical act[s], such as stealing company funds," and much broader claims that may encompass several such acts, such as conspiracy. *In re PE Corp. Sec. Litig.*, 221 F.R.D. 20, 25 (D. Conn. 2003).

In *PE Corporation*, which involved claims by investors that a corporation made materially false and misleading statements, the court held that the complaint's specific allegations of misleading statements constituted the "modicum of objective support" sufficient to permit plaintiffs discovery regarding additional specific instances of misleading statements to support their overarching claim that defendants misrepresented their business strategy. *Id.* Similarly, Plaintiffs' existing allegations regarding Defendants' participation in the conspiracy to

kidnap Isabella are sufficient to permit discovery regarding additional specific instances of Defendants' participation to support Plaintiffs' overarching claims of conspiracy.

Defendants' position would essentially require Plaintiffs to know the details of every fact in this case before engaging in discovery.[3] But such a requirement is at odds with the very purpose of discovery, which is "to find out additional facts about a well-pleaded claim." *Jones v. Capital Cities/ABC, Inc.*, 168 F.R.D. 477, 480 (S.D.N.Y. 1996); *see also Hickman v. Taylor*, 329 U.S. 495, 507 (1947) ("Mutual knowledge of all the relevant facts gathered by both parties is essential to proper litigation. To that end, either party may compel the other to disgorge whatever facts he has in his possession.").

B. Plaintiffs Are Not Engaged in a Fishing Expedition.

Because each of the Requests is supported by the factual allegations of the Complaint and seeks evidence regarding Plaintiffs' existing, well-pleaded claims, Plaintiffs are not engaged in a fishing expedition. A fishing expedition is aimed at finding facts to state a claim that has yet to be adequately asserted. *Bridgewater v. Taylor*, 745 F. Supp. 2d 355, 358 & n.1 (S.D.N.Y 2010) (quoting *KBL Corp. v. Arnouts*, 646 F. Supp. 2d 355, 346 n.6 (S.D.N.Y. 2009)); *see also Podany v. Robertson Stephens, Inc.*, 350 F. Supp. 2d 375, 378 (S.D.N.Y. 2004) ("[D]iscovery is authorized solely for parties to develop the facts in a lawsuit in which a plaintiff has stated a legally cognizable claim, not in order to permit a plaintiff to find out whether he has such a claim . . . .").

[3] This misunderstanding may underlie Defendants' bizarre assertion that Plaintiffs "admitted" that they are engaged in a fishing expedition. Resp. at 7, ECF 374. Plaintiffs made no such admission. Plaintiffs' counsel intended to convey only that Plaintiffs do not know, and cannot be expected to know, the full universe of evidence in Defendants' possession before engaging in discovery.

For example, in *Tottenham*, which involved counterclaims by a defendant-employer based on information that a plaintiff-employee misappropriated company funds in two specific instances, the court rejected the defendant's broad discovery requests concerning the plaintiff's personal financial records based on nothing more than speculation that the plaintiff may have engaged in additional acts of misappropriation. 2002 WL 1967023, at *1–2. Importantly, any additional instances of misappropriation revealed by discovery would have constituted separate claims "beyond those already alleged in the Answer." *Id.* at *2; *accord Gopher Excavation, Inc. v. N. Am. Pipe Corp.*, No. 17-cv-1021, 2017 WL 7355300, at *5 (D. Colo. Dec. 15, 2017) ("Discovery is a fishing expedition when it goes beyond the pleadings' allegations to attempt finding additional violations or claims.").

This Court, by contrast, has already held that Plaintiffs state claims against Defendants for conspiracy to violate Plaintiffs' civil and parental rights. Op. & Order at 35, 62–63, ECF 277. The Requests seek nothing more than evidence to support those well-pleaded claims.

II. The Requests Are Proportional and not Unduly Burdensome.

Defendants fail to meet their burden of demonstrating, with particularized facts discovered through reasonable inquiry, why they should be allowed to withhold documents responsive to the Requests, which are relevant and justified by allegations of the Complaint. *See* Fed. R. Civ. P. 34(b)(2); *see also N. Shore–Long Island Jewish Health Sys., Inc. v. MultiPlan, Inc.*, 325 F.R.D. 36, 48 (E.D.N.Y. 2018) ("Once the requesting party has made a *prima facie* showing of relevance, it is up to the responding party to justify curtailing discovery." (internal quotation marks omitted)); *Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354, 358–59 (D. Md. 2008).

When determining whether discovery requests are proportional to the needs of the case, Rule 26(b)(1) of the Federal Rules of Civil Procedure instructs courts to consider "the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit."

Despite their burden to show that the Requests are disproportional, Defendants' Response only touches on these factors obliquely. A thorough consideration of these factors demonstrates that the Requests are proportional.

First, the issues at stake in this action are important. This case involves a conspiracy to commit international kidnapping that was motivated by animus against gay and lesbian people and was intended to hinder the government in securing them the equal protection of the laws. Count Two of the Complaint states a claim under 42 U.S.C. § 1985(3), which the Reconstruction Congress passed to permit private persons to enforce their right to equal protection against private actors as well as the government. *See, e.g.*, *Griffin v. Breckenridge*, 403 U.S. 88, 98–101 (1971). The Supreme Court has observed that "[u]nlike most private tort litigants, a civil rights plaintiff seeks to vindicate important civil and constitutional rights that cannot be valued solely in monetary terms." *City of Riverside v. Rivera*, 477 U.S. 561, 574 (1986).

Second, Plaintiffs have made several specific claims for damages. *See* Compl. ¶¶ 68–72, ECF 223. Beyond these requests, Jenkins has suffered—and continues to suffer—the loss of her child for the past decade.

Third, the information sought by the Requests is almost entirely in the hands of the Defendants. Indeed, the disparity of information between Defendants and Plaintiffs previously

led this Court to dismiss Plaintiffs' claims against Liberty University based on Defendants' actions. *See* Op. & Order at 26, ECF 220. Plaintiffs only learned of the facts that led to the joinder of Defendants at the criminal trial of their co-conspirator Zodhiates. *Id.*

Fourth, Defendants' allusion to a "$450 million war chest" notwithstanding, Defendants have submitted no evidence on the comparative resources of the parties, as opposed to those of their lawyers. *Cf. Sines v. Kessler*, 325 F.R.D. 563, 568 (2018) (denying motion for protective order in part because "[w]hile plaintiffs' legal representation resources appear superior to movant's, the court has no information concerning the resources of the parties themselves.").

Fifth, the information sought by the Requests goes to the heart of the issues in this case. To prove Count One, for example, Plaintiffs must show that Defendants formed an agreement to interfere with Jenkins's parental rights and took some unlawful action in furtherance of that agreement. *See* Op. & Order at 32, ECF 277. Defendants' communications with and about Jenkins, Isabella, and Lisa Miller are likely to reveal the specifics of Defendants' agreement to become part of the conspiracy as well as the dates and details of their actions in furtherance of the conspiracy. Defendants' communications and information about events that occurred around the dates of the most important events of this case are particularly likely to flesh out Defendants' whereabouts and actions on those dates. *See Sines*, 325 F.R.D. at 568 (denying motion for protective order due to importance of evidence to requesting party's claims).

Finally, the discussion of the first five factors demonstrates why the likely benefit of the information revealed by the Requests outweighs their burden on Defendants. Defendants' attempt to shift this balance is two-fold. First, in their Response—for the first time—Defendants attempt to provide particularized facts about the burden or expense of the proposed discovery, noting that the responsive documents in their possession comprise "17 bankers' boxes of paper

files, comprising over 42,500 pages" and a "15+ gigabyte electronic file, comprising tens of thousands of documents." Resp. at 4–5, ECF 374 (emphasis omitted).[4]

But discovery is frequently an expensive and time-consuming process. *See, e.g., Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 559, 570 (2007) (noting the "potentially enormous expense of discovery" as a basis to require plaintiffs to "state enough facts to state a claim for relief that is plausible on its face" before permitting discovery); *see also Trask v. Olin Corp.*, 298 F.R.D. 244, 266 (W.D. Pa. 2014) (permitting requests that would require producing party to process 270 bankers boxes of information). If burden were the sole consideration, many meritorious cases would likely never proceed past the pleadings stage. See *In re PE Corp.*, 221 F.R.D at 27 ("[T]he court finds that the plaintiffs' interest in full disclosure outweighs the defendants' interest in conserving time and expense.").

Hence Defendants' second contention, that the Requests are unlikely to be beneficial because "most" of the documents are privileged. Resp. at 5, ECF 374. But Plaintiffs' Motion to Compel contains specific examples of the kinds of nonprivileged documents that would be responsive to the Requests. *See* Mot. to Compel at 6, 8–9, ECF 361 (emails between Lindevaldsen and Lisa Miller about Lindevaldsen's book, "encouraging" emails Lisa Miller sent to Lindevaldsen, emails about the "personal option," communications advising Lisa Miller to "disappear"). Though Plaintiffs have significant reason to believe these documents exist, Defendants have yet to produce them. In light of such particularized examples, Defendants' bare

[4] These numbers appear to comprise only Defendants' litigation file related to "massive, multi-jurisdictional custody litigation" between Jenkins and Lisa Miller. Resp. at 4, ECF 374. If this is the case, it bears noting that the case file does not necessarily contain all documents responsive to the Requests. Moreover, Defendants will not be required to produce all documents in that file because Plaintiffs have already agreed to exclude publicly available court filings.

assertion that "most" responsive documents would "likely" be privileged is insufficient to undercut the likely benefit of the information revealed by the Requests.

III. Defendants' Refusal To Produce a Privilege Log Is Unjustified.

Defendants have failed to satisfy their burden of proving that they should be excused from providing a privilege log. *See* Fed. R. Civ. P. 26(b)(5)(A). Plaintiffs have made specific allegations of wrongdoing against Defendants. *See, e.g.*, Compl. ¶ 61, ECF 223. Based on these allegations, Plaintiffs believe that the crime–fraud exception to the attorney–client privilege applies to some portion of Defendants' otherwise privileged documents. *See* Mot. to Compel at 9–10, ECF 361 (quoting *Chevron Corp. v. Salazar*, 275 F.R.D. 437, 451 (S.D.N.Y. 2011)).

Parties may move a trial court to conduct an in camera review of documents when they possess "a factual basis adequate to support a good faith belief by a reasonable person" that the crime–fraud exception applies. *United States v. Zolin*, 491 U.S. 554, 572 (1989). Without this procedure, the crime–fraud exception would be a "dead letter" because the application of the exception to the privilege can only be proved via disclosure of privileged materials. *Id.* at 566 (internal quotation marks omitted). Defendants cannot circumvent this procedure by refusing to produce a privilege log upon which Plaintiffs could base such a showing. *See Netjumper Software, LLC v. Google, Inc.*, No. M19-138, 2005 WL 3046271, at *3 (S.D.N.Y. 2005) ("The purpose of a privilege log is to provide a description of the allegedly privileged materials sufficient to enable the demanding party to challenge the claim of privilege.").

Moreover, Defendants' reliance on cases excusing law firms from providing a privilege log for productions that contain a large volume of privileged communications, Resp. at 10, ECF 374, elides the crucial distinction between those cases and this one: none of those cases involved a law firm as a party accused of illegal activity. Rather, they involved discovery

requests about peripheral matters aimed by one party at the attorneys of another party. *Edmondson v. RCI Hospitality Holdings, Inc.*, No. 16-cv-2242, 2018 WL 4112816, at *1 (S.D.N.Y. Aug. 29, 2018), for example, involved a privacy dispute between various clubs and their dancers. The dancers served discovery requests for all communications between the clubs' attorneys and the attorneys in similar lawsuits, which the court denied as irrelevant. 2018 WL 4112816, at *2. The court also noted that the attorneys were not required to create a privilege log because the documents were not "otherwise discoverable" and were likely covered by the attorney–client privilege. *Id.* n.2.

Liberty Counsel and Lindevaldsen, by contrast, are named defendants, and the Requests solicit evidence that bears on the issues at the heart of this case. Defendants should be ordered to comply with their responsibility to provide Plaintiffs with a privilege log.

IV. Defendants' Communications over Liberty University's Email Server Are Not Privileged.

Plaintiffs' challenge to Defendants' assertion of privilege over the documents in Liberty University's possession further indicates that Defendants' blanket privilege assertion is flawed. On June 18, 2019, Defendants served Plaintiffs with a document-by-document privilege log for 82 documents responsive to Plaintiffs' subpoena to Liberty University over which Defendants asserted the attorney–client privilege. Clemons Decl. ¶ 2. Liberty University must have provided those documents to Defendants' counsel in order for counsel to create the privilege log, placing those documents within Defendants' possession, custody, or control. Plaintiffs' challenge to Defendants' privilege assertion over these specific documents is therefore ripe for review.

Defendants' own authorities acknowledge that an employee cannot have a reasonable expectation of privacy sufficient to sustain the attorney–client privilege on a continually monitored employer email server. *See* Resp. at 12–13, ECF 374 (citing *Leventhal v. Knapek*, 266

F.3d 64, 73–74 (2d Cir. 2001), for the proposition that an "employee had reasonable expectation of privacy in emails . . . *where the employer did not have a practice of regularly reviewing the contents of employee's computers*" (emphasis added)). But Liberty University explicitly states in its "Acceptable Use Policy," which Defendants were required to read and acknowledge, that:

> No user of University systems should have an expectation of privacy in their electronic communications. All electronic communications . . . presented to and/or passed in the Liberty network . . . may be monitored, examined, saved, read, transcribed, stored, or re-transmitted by an authorized employee or agent of the University, in its sole discretion, with or without prior notice to the user. The University reserves *and intends to exercise* the right to do so.

Liberty Univ. Acceptable Use Policy at 5–6, ECF 361-7 (emphasis added).

In *Scott v. Beth Israel Medical Center, Inc.*, 847 N.Y.S.2d 436, 439 (N.Y. Sup. Ct. 2007), a New York court evaluated a similar policy that stated that "[e]mployees have no personal privacy right in any material created, received, saved or sent using [employer] communication or computer systems," and that "[t]he [employer] reserves the right to access and disclose such material at any time without prior notice." The court ruled that use of the system waived the attorney–client privilege under New York law because the policy created the same effect as "the employer looking over your shoulder each time you send an e-mail." *Id.* at 440.

Furthermore, clinical education at American law schools would survive a holding that Defendants' use of the Liberty University email server waived the attorney–client privilege for two reasons. First, the acceptable use policies of many law schools are not as intrusive as Liberty University's policy. *See, e.g.*, Harvard Law School, *Policy on Access to Electronic Information* at 3, Ex. 2 ("The University does not routinely monitor the content of information transmitted through or stored in University information systems."); Yale Law School, *Information Technology Appropriate Use Policy* at 6, Ex. 3 (listing only six specific conditions under which

university officials will access user information without consent and outlining specific procedures for doing so).[5] Moreover, other clinics likely do not share the unique relationship of Liberty Counsel and Liberty University, which, they assert, "are legally and corporately separate and distinct entities" headquartered in different cities in different states. Mem. in Supp. of Defs. Liberty Counsel, Mathew Staver, and Rena Lindevaldsen's Mot. to Dismiss at 2, ECF 240.

V. The Requests Do Not Implicate Defendants' First Amendment Rights.

Defendants' reliance on the First Amendment associational privilege articulated in *NAACP v. Alabama*, 357 U.S. 449 (1958), stretches that privilege beyond recognition. That is because *NAACP* itself, as well as every other Supreme Court decision cited by Defendants, privileged the disclosure of the *membership lists* of local NAACP chapters. *See NAACP*, 357 U.S. at 462; *see also Gibson v. Fla. Legislative Investigative Comm.*, 372 U.S. 539, 543–44 (1963) (reversing contempt conviction for failure to disclose NAACP membership lists to subversive activities committee); *Bates v. City of Little Rock*, 361 U.S. 516, 523–25 (1960) (same). Indeed, Defendants cut off their block quotation of *Sherwin-Williams Company v. Spitzer* immediately before the court's observation that "[t]ypically, the association privilege has been enforced to protect an organization's internal activities and documents, *such as lists of members, contributors, and political affiliations*." No. 1:04-cv-185, 2005 WL 2128938, at *4 (N.D.N.Y. Aug. 24, 2005) (emphasis added) (evaluating whether an association could be compelled to turn over its membership list).

The Requests do not seek anything resembling a membership list from Defendants. Rather, they seek evidence directly relevant to proving Defendants' animus against LGBT

[5] Harvard Law School also creates unique email accounts for its clinics and informs students that they "should not use their personal email account or their regular HLS student account for externship or pro bono work." Harvard Law School, *Clinical Policies & FAQ* at 9, Ex. 4.

individuals, which is an element of Count Two. *See* Op. & Order at 50, ECF 277 (citing *Griffin*, 403 U.S. at 102). This Court, quoting *Obergefell v. Hodges*, 135 S. Ct. 2584, 2598 (2015), has explicitly noted that opposition to same-sex marriage demeans gays and lesbians. *Id.* at 16.

Defendants contend that requiring them to disclose their beliefs about same-sex marriage in discovery contradicts a different portion of *Obergefell*, which ensures that "those who adhere to religious doctrines[] may continue to advocate with utmost, sincere conviction that . . . same-sex marriage should not be condoned." Resp. at 17, ECF 374 (quoting *Obergefell*, 135 S. Ct. at 2607).[6] Once again, Defendants' reliance on this passage falsely equates their own conduct and that of others—in this case, other opponents to same-sex marriage. The First Amendment guarantees the right to possess and express the belief that "same-sex marriage should not be condoned"; it does not guarantee the right to engage in a conspiracy to kidnap a girl from her mother based on that belief.

As the Court has previously observed in this case, Section 1985(3) does not prohibit the possession or even the expression of animus, but rather *actions motivated by animus* that hinder authorities in providing Plaintiffs with equal protection of the laws. Op. & Order at 96, ECF 277. Under Defendants' theory, the First Amendment would always prohibit discovery of evidence regarding motive. For example, there is a First Amendment right to possess and express the belief that billionaires should be robbed. *See Brandenburg v. Ohio*, 395 U.S. 444 (1969). But the robber surely has no First Amendment privilege to prevent discovery of those expressions as

[6] Tellingly, Defendants' only response to Plaintiffs' observation that Defendants themselves have disclosed similar information for decades is to question why the Requests are necessary if such information is so well-known. Resp. at 16, ECF 374. As lawyers themselves, Defendants should be well aware of the difference between a fact that "everyone knows" and authenticated evidence that can be used to prove an issue in a court of law. *See* 8 Charles Wright & Arthur R. Miller, *Federal Practice and Procedure* § 2014 (4th ed. 2010) (parties are allowed to seek discovery about matters already within their knowledge).

evidence of motive when on trial for actually robbing a billionaire. *See Giboney v. Empire Storage & Ice Co.*, 336 U.S. 490, 498 (1949).

For the same reason, compelling Defendants to produce documents responsive to the Requests will not chill debate about same-sex marriage any more than robbery prosecutions chill discussions about class warfare. So long as same-sex marriage opponents do not engage in a conspiracy to kidnap that hinders state authorities, they have nothing to fear from this Court requiring Defendants to comply with the Requests.

CONCLUSION

For these reasons, Plaintiffs' motion to compel should be granted.

September 24, 2019

Respectfully submitted.

/s/
J. Tyler Clemons
Southern Poverty Law Center
201 St. Charles Avenue, Suite 2000
New Orleans, Louisiana 70170
Phone: (504) 526-1530
Fax: (504) 486-8947
Email: tyler.clemons@splcenter.org

/s/
Frank H. Langrock
Langrock Sperry & Wool, LLP
111 S. Pleasant Street
P.O. Drawer 351
Middlebury, Vermont 05753-0351
Phone: (802) 388-6356
Fax: (802) 388-6149
Email: flangrock@langrock.com

Sarah Star
Sarah Star, PL
P.O. Box 106
Middlebury, Vermont 05753
Phone: (802) 385-1023
Email: srs@sarahstarlaw.com

David C. Dinielli
Diego A. Soto
Southern Poverty Law Center
400 Washington Avenue
Montgomery, Alabama 36104
Phone: (334) 956-8200
Fax: (334) 956-8481
Email: david.dinielli@splcenter.org
Email: diego.soto@splcenter.org

Counsel for Plaintiffs

Exhibit 1

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF VERMONT

JANET JENKINS, ET AL., Plaintiffs, v. KENNETH L. MILLER, ET AL. Defendants.	Docket No. 2:12-CV-00184

LOG OF PRIVILEGE ASSERTIONS BY LIBERTY COUNSEL, MATHEW STAVER AND RENA LINDEVALDSEN OVER PLAINTIFF'S SUBPOENA TO NON-PARTY LIBERTY UNIVERSITY

Liberty Counsel, Mathew Staver and Rena Lindevaldsen assert the following privileges over the following documents identified by non-party Liberty University as potentially responsive to Plaintiff Janet Jenkins' subpoena directed Liberty University dated October 31, 2018:

No	Document Type [Control Number]	Date(s) of Document	Author(s)	Recipient(s)	Subject	Privilege Asserted
1.	Correspondence [DOC-001]	7/7/2008	Steve Crampton	Steve Crampton; Rena Lindevaldsen; David Corry; Mathew Staver; Norman C. Smith; Bonnie Gentry (paralegal)	Email chain between counsel and paralegal discussing strategy for hearing in Miller/Jenkins litigation.	Work Product
2.	Correspondence [DOC-002]	7/7/2008	Rena Lindevaldsen	Steve Crampton; Rena Lindevaldsen; David Corry; Mathew Staver; Norman C. Smith	Email chain between counsel discussing strategy for hearing in Miller/Jenkins litigation.	Work Product
3.	Correspondence [DOC-003]	7/7/2008	David Corry	Steve Crampton; Rena Lindevaldsen; David Corry; Mathew Staver; Norman C. Smith	Email chain between counsel discussing strategy for hearing in Miller/Jenkins litigation.	Work Product

4.	Correspondence [DOC-004]	7/10/2007	David Corry	Norman C. Smith; Rena Lindevaldsen; Erik Stanley; Steve Crampton; Mathew Staver	Email chain between counsel discussing appeal in Miller/Jenkins litigation.	Work Product
5.	Correspondence [DOC-005]	6/29/2007	David Corry	Rena Lindevaldsen	Email discussing documents to be filed in Miller/Jenkins litigation.	Work Product
6.	Correspondence [DOC-006]	6/8/2007	David Corry	Rena Lindevaldsen; Erik Stanley; Steve Crampton; Mathew Staver	Email chain discussing documents to be filed in Miller/Jenkins litigation.	Work Product
7.	Draft Pleading [DOC-007]	6/8/2007	Liberty Counsel	N/A	Draft document to be filed in Miller/Jenkins litigation.	Work Product
8.	Correspondence [DOC-008]	5/3/2007	Tessa Sturgill, communications director at Liberty Counsel	Rena Lindevaldsen; Mathew Staver; Anita Staver	Email discussing media strategy for legal issues in Miller/Jenkins litigation.	Work Product
9.	Correspondence [DOC-009]	3/26/2007	Gary Kreep, allied counsel at United States Justice Foundation ("USJF")	Stephen Crampton; Rena Lindevaldsen; Mathew Staver; USJF staff	Email discussing communications with joint client and trial strategy in Miller/Jenkins litigation.	Attorney-Client/ Work Product
10.	Correspondence [DOC-010]	3/26/2007	Erik Stanley	Mathew Staver; Rena Lindevaldsen	Email discussing potential joint representation with USJF in Miller/Jenkins litigation.	Work Product
11.	Correspondence [DOC-011]	3/20/2007	David Corry	Mathew Staver; Rena Lindevaldsen; Erik Stanley	Email discussing potential joint representation with USJF in Miller/Jenkins litigation.	Work Product
12.	Correspondence [DOC-012]	3/19/2007	David Corry	Mathew Staver; Rena Lindevaldsen; Lisa Miller; Belinda Wetherington, office manager at Liberty Counsel	Email communications with client and among counsel regarding documents to be filed, and litigation strategy, in Miller/Jenkins litigation.	Attorney-Client/ Work Product
13.	Correspondence [DOC-013]	3/19/2007	Belinda Wetherington	David Corry; Rena Lindevaldsen; Mathew Staver; Lisa Miller	Email communications with client and among counsel regarding documents to be filed, and litigation strategy, in Miller/Jenkins litigation.	Attorney-Client/ Work Product
14.	Correspondence [DOC-014]	3/19/2007	David Corry	Lisa Miller; Belinda Wetherington; Rena Lindevaldsen; Norman C. Smith; Mathew Staver	Email communication with client regarding documents to be filed, and litigation strategy, in Miller/Jenkins litigation.	Attorney-Client/ Work Product
15.	Draft Pleading [DOC-015]	6/8/2007	Liberty Counsel	N/A	Draft document to be filed in Miller/Jenkins litigation.	Work Product
16.	Correspondence [DOC-016]	3/9/2007	David Corry	Belinda Wetherington; Rena Lindevaldsen; Mary McAlister; Mathew Staver; Anita Staver	Email chain discussing strategy and timing for Miller/Jenkins litigation.	Work Product
17.	Correspondence [DOC-017]	2/12/2007	Belinda Wetherington	Rena Lindevaldsen; David Corry; Mary McAlister; Mathew Staver; Anita Staver	Email chain discussing client contact, communications and preparations for Miller/Jenkins litigation.	Work Product

18.	Correspondence [DOC-018]	2/8/2007	Lisa Miller	Rena Lindevaldsen	Email discussing media articles and communications relative to ongoing Miller/Jenkins litigation.	Attorney-Client/ Work Product
19.	Correspondence [DOC-019]	2/8/2007	Belinda Wetherington	Rena Lindevaldsen	Email discussing documents to be filed and sent to client in Miller/Jenkins litigation.	Work Product
20.	Correspondence [DOC-020]	2/7/2007	Lisa Miller	Rena Lindevaldsen	Email chain discussing strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
21.	Correspondence [DOC-021]	2/6/2007	Lisa Miller	Rena Lindevaldsen	Email discussing strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
22.	Correspondence [DOC-022]	2/4/2007	Lisa Miller	Rena Lindevaldsen	Email chain discussing facts and strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
23.	Correspondence [DOC-023]	2/3/2007	Lisa Miller	Rena Lindevaldsen	Email chain discussing facts and strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
24.	Correspondence [DOC-024]	2/3/2007	Lisa Miller	Rena Lindevaldsen	Email chain discussing facts and strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
25.	Correspondence [DOC-025]	2/3/2007	Lisa Miller	Rena Lindevaldsen	Email chain discussing facts and strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
26.	Correspondence [DOC-026]	1/30/2007	Lisa Miller	Rena Lindevaldsen	Email discussing contact with potential witnesses in Miller/Jenkins litigation.	Attorney-Client/ Work Product
27.	Correspondence [DOC-027]	1/28/2007	Lisa Miller	Rena Lindevaldsen	Email providing update in Miller/Jenkins litigation.	Attorney-Client/ Work Product
28.	Correspondence [DOC-028]	1/15/2007	Lisa Miller	Rena Lindevaldsen	Email discussing facts and strategy for Miller/Jenkins litigation.	Attorney-Client / Work Product
29.	Correspondence [DOC-029]	1/15/2007	Lisa Miller	Rena Lindevaldsen	Email discussing facts and strategy for Miller/Jenkins litigation.	Attorney-Client / Work Product
30.	Correspondence [DOC-030]	1/8/2007	Lisa Miller	Rena Lindevaldsen	Email discussing strategy for hearing in Miller/Jenkins litigation.	Attorney-Client/ Work Product
31.	Correspondence [DOC-031]	12/12/2006	Lisa Miller	Rena Lindevaldsen	Email discussing facts and strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
32.	Correspondence [DOC-032]	12/10/2006	Lisa Miller	Rena Lindevaldsen; Erik Stanley; Belinda Wetherington	Email chain discussing facts and strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
33.	Correspondence [DOC-033]	11/30/2006	Lisa Miller	Rena Lindevaldsen; Mathew Staver; Rena Lindevaldsen; Susan Jacobus, receptionist at Liberty Counsel	Email chain discussing facts and strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
34.	Correspondence [DOC-034]	11/18/2006	Lisa Miller	Rena Lindevaldsen	Email discussing facts and strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
35.	Correspondence [DOC-035]	11/17/2006	Lisa Miller	Rena Lindevaldsen; Belinda Wetherington	Email chain discussing update and strategy in Miller/Jenkins litigation.	Attorney-Client/ Work Product
36.	Correspondence [DOC-036]	11/17/2006	Lisa Miller	Rena Lindevaldsen; Belinda Wetherington	Email chain discussing update and strategy in Miller/Jenkins litigation.	Attorney-Client/ Work Product
37.	Correspondence [DOC-037]	11/17/2006	Lisa Miller	Rena Lindevaldsen; Belinda Wetherington	Email chain discussing update and strategy in Miller/Jenkins litigation.	Attorney-Client/ Work Product

38.	Correspondence [DOC-038]	11/15/2006	Lisa Miller	Rena Lindevaldsen; Belinda Wetherington	Email chain discussing update and strategy in Miller/Jenkins litigation.	Attorney-Client/ Work Product
39.	Correspondence [DOC-039]	11/13/2006	Lisa Miller	Rena Lindevaldsen	Email discussing strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
40.	Correspondence [DOC-040]	11/12/2006	Lisa Miller	Rena Lindevaldsen	Email discussing facts and strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
41.	Correspondence [DOC-041]	10/28/2006	Lisa Miller	Rena Lindevaldsen	Email chain discussing update, facts and strategy in Miller/Jenkins litigation.	Attorney-Client/ Work Product
42.	Correspondence [DOC-042]	10/26/2006	Lisa Miller	Rena Lindevaldsen	Email chain discussing update, facts and strategy in Miller/Jenkins litigation.	Attorney-Client/ Work Product
43.	Correspondence [DOC-043]	10/26/2006	Lisa Miller	Rena Lindevaldsen	Email chain discussing update, facts and strategy in Miller/Jenkins litigation.	Attorney-Client/ Work Product
44.	Correspondence [DOC-044]	9/27/2006	Lisa Miller	Rena Lindevaldsen	Email chain discussing facts and strategy for Miller/Jenkins litigation..	Attorney-Client/ Work Product
45.	Correspondence [DOC-045]	5/6/2009	Rena Lindevaldsen	Rena Lindevaldsen	Email note-to-self regarding documents to be filed in Miller/Jenkins litigation.	Work Product
46.	Correspondence [DOC-046]	2/8/2007	Rena Lindevaldsen	Belinda Wetherington	Email chain discussing documents to be filed and sent to client in Miller/Jenkins litigation.	Work Product
47.	Correspondence [DOC-047]	2/7/2007	Rena Lindevaldsen	Lisa Miller	Email chain discussing strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
48.	Correspondence [DOC-048]	2/6/2007	Rena Lindevaldsen	Lisa Miller	Email chain discussing strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
49.	Correspondence [DOC-049]	1/30/2007	Rena Lindevaldsen	Lisa Miller	Email discussing contact with potential witnesses in, and strategy for, Miller/Jenkins litigation.	Attorney-Client/ Work Product
50.	Scheduling Note [DOC-050]	6/21/2010	Candy McGuire, Liberty Counsel secretary	Mat Staver	Scheduling Note regarding preparation efforts and strategy for Miller/Jenkins litigation	Work Product
51.	Scheduling Note [DOC-051]	6/2/2010	Bonnie Gentry	Mat Staver	Scheduling Note regarding preparation efforts and strategy for Miller/Jenkins litigation.	Work Product
52.	Scheduling Note [DOC-052]	2/12/2010	Mathew Staver	Mathew Staver	Scheduling Note regarding preparation efforts and strategy for Miller/Jenkins litigation.	Work Product
53.	Scheduling Note [DOC-053]	2/12/2010	Mathew Staver	Mathew Staver	Scheduling Note regarding preparation efforts and strategy for Miller/Jenkins litigation.	Work Product
54.	Scheduling Note [DOC-054]	1/15/2010	Mathew Staver	Mathew Staver	Scheduling Note regarding preparation efforts and strategy for Miller/Jenkins litigation.	Work Product
55.	Scheduling Note [DOC-055]	12/22/2009	Mathew Staver	Mathew Staver	Scheduling Note regarding preparation efforts and strategy for Miller/Jenkins litigation.	Work Product
56.	Scheduling Note [DOC-056]	12/22/2009	Mathew Staver	Mathew Staver	Scheduling Note regarding preparation efforts and strategy for Miller/Jenkins litigation.	Work Product
57.	Scheduling Note [DOC-057]	12/7/2009	Mathew Staver	Mathew Staver	Scheduling Note regarding preparation efforts and strategy for Miller/Jenkins litigation.	Work Product

58.	Scheduling Note [DOC-058]	8/10/2009	Mathew Staver	Mathew Staver	Scheduling Note regarding preparation efforts and strategy for Miller/Jenkins litigation.	Work Product
59.	Scheduling Note [DOC-059]	6/8/2009	Mathew Staver	Mathew Staver	Scheduling Note regarding client contact and strategy for Miller/Jenkins litigation.	Work Product
60.	Correspondence [DOC-060]	8/22/2006	Mathew Staver	Rena Lindevaldsen; Anita Staver	Email chain regarding strategy for Miller/Jenkins litigation.	Work Product
61.	Correspondence [DOC-061]	10/18/2006	Mathew Staver	Anita Staver; Erik Stanley; Rena Lindevaldsen	Email chain regarding strategy for Miller/Jenkins litigation.	Work Product
62.	Correspondence [DOC-062]	7/3/2009	Lisa Miller	Rena Lindevaldsen	Email providing evidence for use in Miller/Jenkins litigation.	Attorney-Client
63.	Correspondence [DOC-063]	6/25/2009	Lisa Miller	Rena Lindevaldsen	Email discussing case update about Miller/Jenkins litigation.	Attorney-Client/ Work Product
64.	Correspondence [DOC-064]	6/6/2009	Lisa Miller	Rena Lindevaldsen	Email chain discussing facts and strategy for Miller/Jenkins litigation.	Attorney-Client / Work Product
65.	Correspondence [DOC-065]	6/6/2009	Lisa Miller	Rena Lindevaldsen	Email chain discussing strategy, status and developments in Miller/Jenkins litigation.	Attorney-Client / Work Product
66.	Correspondence [DOC-066]	6/5/2009	Lisa Miller	Rena Lindevaldsen	Email chain discussing strategy for Miller/Jenkins litigation.	Attorney-Client / Work Product
67.	Correspondence [DOC-067]	6/5/2009	Lisa Miller	Rena Lindevaldsen	Email chain discussing strategy for Miller/Jenkins litigation.	Attorney-Client / Work Product
68.	Correspondence [DOC-068]	5/29/2009	Lisa Miller	Rena Lindevaldsen; Steve Crampton; Mathew Staver; Matthew Barber; Horatio Mihet	Email chain discussing developments in and strategy for Miller/Jenkins litigation.	Attorney-Client / Work Product
69.	Correspondence [DOC-069]	5/28/2009	Lisa Miller	Rena Lindevaldsen; Steve Crampton; Mathew Staver; Matthew Barber; Horatio Mihet	Email chain discussing developments in and strategy for Miller/Jenkins litigation.	Attorney-Client / Work Product
70.	Correspondence [DOC-070]	5/27/2009	Lisa Miller	Rena Lindevaldsen; Steve Crampton; Mathew Staver; Matthew Barber; Horatio Mihet	Email chain discussing developments in and strategy for Miller/Jenkins litigation.	Attorney-Client / Work Product
71.	Correspondence [DOC-071]	2/11/2009	Lisa Miller	Rena Lindevaldsen	Email discussing strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
72.	Correspondence [DOC-072]	2/10/2009	Lisa Miller	Rena Lindevaldsen	Email discussing strategy for Miller/Jenkins litigation.	Attorney-Client/ Work Product
73.	Correspondence [DOC-073]	2/10/2009	Lisa Miller	Rena Lindevaldsen	Draft letter regarding Virginia law and legal system in regards to Miller/Jenkins litigation.	Attorney-Client / Work Product
74.	Correspondence [DOC-074]	5/29/2008	Lisa Miller	Rena Lindevaldsen; Steve Crampton; Mathew Staver	Email regarding potential testimony in Miller/Jenkins litigation.	Attorney-Client
75.	Correspondence [DOC-075]	5/29/2008	Lisa Miller	Rena Lindevaldsen; Steve Crampton; Mathew Staver	Email regarding potential testimony in Miller/Jenkins litigation.	Attorney-Client
76.	Correspondence [DOC-076]	2/7/2009	Lisa Miller	Rena Lindevaldsen	Email discussing strategy for Miller/Jenkins litigation.	Attorney-Client
77.	Scheduling Note [DOC-077]	11/13/2009	Candy McGuire	Mathew Staver	Scheduling note regarding hearing in Miller/Jenkins litigation.	Work Product

78.	Scheduling Note [DOC-078]	11/12/2009	Mathew Staver	Mathew Staver	Scheduling note regarding hearing in Miller/Jenkins litigation.	Work Product
79.	Scheduling Note [DOC-079]	11/12/2009	Candy McGuire	Mathew Staver	Scheduling note regarding hearing in Miller/Jenkins litigation.	Work Product
80.	Scheduling Note [DOC-080]	11/12/2009	Candy McGuire	Mathew Staver	Scheduling note regarding hearing in Miller/Jenkins litigation.	Work Product
81.	Scheduling Note [DOC-081]	11/12/2009	Mathew Staver	Mathew Staver	Scheduling note regarding hearing in Miller/Jenkins litigation.	Work Product
82.	Scheduling Note [DOC-082]	2/17/2010	Mathew Staver	Mathew Staver	Scheduling note regarding hearing in Miller/Jenkins litigation.	Work Product
83.	Correspondence UNIV-01796	11/12/2009	Amanda Haas	Various recipients at Liberty University	Invitation to private luncheon with Congressman Trent Franks	Names and emails of educational recipients redacted for educational privacy and lack of relevance
84.	Scheduling Note UNIV-01811	11/11/2009	Beverly Smith	Mathew Staver	Appointment with law student to discuss possible withdrawal	Last name of student redacted for educational privacy and lack of relevance
85.	Scheduling Note UNIV-01816	11/9/2009	Barbara Baxter	Mathew Staver and other LU personnel	Meeting to discuss faculty appointments	Candidate information redacted for educational and personnel privacy and lack of relevance
86.	Correspondence UNIV-01833	11/9/2009	Mathew Staver	ABA personnel	Communication regarding ABA site visit at LUSOL	Names and emails of ABA personnel redacted per ABA confidentiality requirements and lack of relevance
87.	Correspondence UNIV-01919	1/27, 2/8-9/2009	Lisa Miller	Joe	Facebook conversation	Profile picture, last name and medical conditions of recipient redacted for medical privacy and lack of relevance
88.	Memorandum UNIV-00336 – UNIV-00339	Summer 2010	Rena Lindevaldsen	Self and/or litigation clinic students subject to confidentiality agreements	Research memorandum disclosing thoughts, impressions and strategy of counsel for Miller/Jenkins and Trudeau litigation.	Work Product

Dated: June 18, 2019.

/s/ Horatio G. Mihet

Horatio G. Mihet
Daniel J. Schmid
Roger K. Gannam
LIBERTY COUNSEL
P.O. Box 540774
Orlando, FL 32854
Phone: (407) 875-1776
Fax: (407) 875-0770
Email: hmihet@lc.org

Attorneys for Defendants Liberty Counsel and Rena Lindevaldsen

CERTIFICATE OF SERVICE

I hereby certify that on this 18th day of June, 2019, a true and correct copy of the foregoing Privilege Log was served via electronic mail on all counsel of record for Plaintiff and Defendants, including:

Beth D. Jacob, Esq. (beth.jacob@splcenter.org)
David C. Dinielli, Esq. (david.dinielli@splcenter.org)
Diego A. Soto, Esq. (diego.soto@splcenter.org)
J. Tyler Clemons, Esq. (Tyler.Clemons@splcenter.org)
Frank H. Langrock, Esq. (flangrock@langrock.com)
Sarah Star, Esq. (srs@sarahstarlaw.com)

Counsel for Plaintiff Janet Jenkins

Brooks G. McArthur, Esq. (bmcarthur@jarvismcarthur.com)

Counsel for Defendant Kenneth L. Miller

Michael J. Tierney, Esq. (mtierney@wadleighlaw.com)

Counsel for Defendant Timothy D. Miller

Robert B. Hemley, Esq. (rhemley@gravelshea.com)

Counsel for Defendants Response Unlimited, Inc., Philip Zodhiates, and Victoria Hyden

Norman C. Smith, Esq. (nc.smith@myfairpoint.net)

Counsel for Defendant Linda Wall

And to:

Liberty University
c/o: Calvin W. Fowler, Jr., Esq. (wfowler@williamsmullen.com)
Harold E. Johnson, Esq. (hjohnson@williamsmullen.com)
Justin S. Feinman, Esq. (jfeinman@williamsmullen.com)

/s/ Horatio G. Mihet
Horatio G. Mihet

Attorney for Defendants Liberty Counsel and Rena Lindevaldsen

Exhibit 2

Policy on Access to Electronic Information

As voted by the President and Fellows of Harvard College on March 31, 2014; amended May 8, 2015

Scope of Policy

This policy sets out guidelines and processes for University access to user electronic information stored in or transmitted through any University system. This policy applies to all Schools and units of the University.

General Statement

Members of the Harvard community rely on technology in multiple aspects of their work, teaching, research, study, and other activity. In doing so, they use electronic systems, networks, and devices that the University owns, provides, or administers. The University makes these systems available for the purpose of carrying out the University's various activities. To promote trust within the University community, the University should be transparent about its policy regarding the circumstances in which it may access user electronic information stored in or transmitted through these systems. This policy therefore sets out guidelines and processes that apply when the University seeks access to such electronic information, consonant with the University's interest in maintaining an environment in which free academic inquiry thrives. This policy is intended to establish internal standards and procedures governing such access by the University; it is not meant to create rights in any individual to seek legal redress for action inconsistent with the policy.

The policy is grounded on six important principles:

- Access should occur only for a legitimate and important University purpose.
- Access should be authorized by an appropriate and accountable person.
- In general, notice should be given when user electronic information will be or has been accessed.
- Access should be limited to the user electronic information needed to accomplish the purpose.
- Sufficient records should be kept to enable appropriate review of compliance with this policy.
- Access should be subject to ongoing, independent oversight by a committee that includes faculty representation.

Terminology

The following terms are used in this policy with the following meanings:

"University systems" refers to all services, networks, and devices owned, provided, or administered by any unit of the University, such as email services, Internet access, file servers, voice message services, storage devices and services, laptop and desktop computers, phones and other mobile devices, and usage and access logs.

"Users" refers to Harvard faculty, others holding academic appointments at Harvard, students, staff, and other employees.

"User electronic information," for any particular user, refers to:

(i) Documents and communications, including emails, voice mails and text messages, and their associated metadata, which are located in files and accounts associated with a particular user. For example, this would include all emails and their attachments in a user's inbox, sent items folder, or other email folders that are recognized as part of the account associated with that user, and all documents in that user account's document folders; and

(ii) Information generated by automated processes triggered by that user's use of University systems, such as tracks of Internet use and logs of access to facilities.

User electronic information does not include (a) records regularly maintained by the University in the ordinary course of business, such as personnel records or student academic records, or information provided by personnel in connection with regular University record-keeping, such as entries in a University travel registry; or (b) information as described in (ii), above, when accessed by the University without identifying or seeking to identify any particular user.

Contents

I. Reasons for Access

The University does not routinely monitor the content of information transmitted through or stored in University information systems. The University may obtain access to user electronic information in some circumstances, but only for a legitimate institutional purpose. The paragraphs below describe certain purposes for which the University may access such information. While this list is expected to cover most instances of access, the list is not intended to be exhaustive. The University may access user electronic information for comparable reasons that likewise advance a legitimate institutional purpose, as determined by a person designated to authorize access pursuant to this policy and subject to review by the oversight committee as described in Part VI.

Although this policy applies to the electronic information of faculty, staff, and students alike, in evaluating the institutional purpose, the person designated to authorize access should in each case weigh not only the stated reasons for access but also the possible effect of access on University values such as academic freedom and internal trust and confidence.

- System Protection, Maintenance, and Management

  University systems require ongoing maintenance and inspection to ensure that they are operating properly; to protect against threats such as attacks, malware, and viruses; and to protect the integrity and security of information. University systems also require regular management, for example, in order to implement new software or other facilities. To do this work, the University may scan or otherwise access user electronic information.

- Business Continuity

  User electronic information may be accessed for the purpose of ensuring continuity in business operations. This need can arise, for example, if an employee who typically has access to the files in question is unavailable due to illness or vacation.

- Safety Matters

  The University may access user electronic information to deal with exigent situations presenting threats to the safety of the campus or to the life, health, or safety of any person.

- Legal Process and Litigation

The University may access user electronic information in connection with threatened or pending litigation, and to respond to lawful demands for information in law enforcement investigations, other government investigations, and legal processes.

- Internal Investigations of Misconduct

The University may access user electronic information in connection with investigations of misconduct by members of the University community, but only when the authorizing person, after weighing the need for access with other University values, has determined that such investigation would advance a legitimate institutional purpose and that there is a sufficient basis for seeking such access. As described in Section VI of this policy, all decisions to access user electronic information are subject to review by an Oversight Committee.

This policy does not apply to reviews of research misconduct allegations conducted under established School-based policies.

II. Authorization of Access

Access to user electronic information should be authorized by an appropriate person, as set forth below. In deciding whether to approve access, the authorizing person should consider whether effective alternative means to obtain the information are reasonably and timely available. In all cases, access must comply with applicable legal requirements.

Authorization for access to user electronic information may be provided by the consent of the user.

Other cases should be handled as follows:

- If the user is a faculty member or other holder of an academic appointment at Harvard, the dean of the relevant Faculty must authorize access.
- If the user is an employee other than a faculty member: (1) the human resources officer or his/her designee for the relevant School or administrative unit must authorize access in business continuity cases; and (2) the dean of the relevant Faculty or the senior administrator of the relevant unit if not a Faculty, or their designees, must authorize access in investigative or other cases.
- If the user is a student, the School-level dean or the dean's designee must authorize access.

Any authorization of access shall apply only to the particular situation and user or users. Any other instance of access must be separately authorized.

No independent authorization is required for information technology personnel to conduct routine system protection, maintenance, or management purposes in accord with internal protocols and processes. Likewise, requests for access in connection with litigation, legal processes, or law enforcement investigations, or to preserve user electronic information for possible subsequent access in accordance with this policy, need no independent authorization if made by the Office of the General Counsel.

In exigent situations involving a threat to campus safety or the life, health, or safety of any person, access may be authorized by the Office of the General Counsel. If emergency conditions do not allow for prior authorization, the matter shall be reported to the Office of the General Counsel as promptly as possible.

For some requests to search user electronic data, it may not be possible to identify any particular user in advance. For example, requests for logs of access to a University facility (swipe card data) often are intended to find out who entered a facility during a particular period; in such cases, the requestor cannot identify a particular user or users because the goal of the search is to learn those identities. Such data requests may still be subject to one of the prior provisions of this Section II, for example, those relating to law enforcement investigations or emergencies. Otherwise, such data search requests must be authorized by the dean of the relevant Faculty or the senior administrator of the relevant unit if not a Faculty, or their designees, in the School or unit where the requestor works.

III. Notice

When the University intends to access user electronic information, notice ordinarily should be given to that user. All reasonable efforts should be made to give notice at the time of access or as soon thereafter as reasonably possible.

System protection, maintenance, and management — Individual notice is not required for ordinary system protection, maintenance, or management. Notice should be given if the access relates specifically to the activity of an individual user.

Business continuity — Individual notice is not required for access to user electronic information for purposes of business continuity, in accordance with established University practice and the common understanding that individual notice in such cases is typically not practical.

Legal restrictions — Individual notice is not required where the University is subject to legal constraints on its ability to give notice.

Emergencies and other extraordinary cases — Contemporaneous notice is not required in cases where there is insufficient time, where giving notice would otherwise interfere with an effective response to an emergency or other compelling need (e.g., at a stage of an internal investigation where giving notice may compromise the investigation), or where it is impractical (e.g., in the case of a former employee). The decision not to give contemporaneous notice must be made by the person designated by this policy to authorize the access. In such cases, notice will ordinarily be given as soon as practical.

The person designated by this policy to authorize access may decide not to give notice. Any such decision, and the reasons for it, shall be described in the records described in Part V of this policy and may be reviewed by the oversight committee, as set forth in Part VI.

IV. Scope of Access

The University shall adopt reasonable steps, whenever practicable, to limit access obtained under this policy to user electronic information that is related to the University's purpose in obtaining access. These steps will vary depending on the circumstances of the search and may include, by way of illustration, designing searches to find specifically designated items, as opposed to categories of information.

Participation in the search, and access to the information, should be limited to those personnel with a reasonable need to be involved.

V. Records of Process

Any person who authorizes access to user electronic information shall provide that reasonable records of the decision process and the reasons for the decision are made and preserved.

The persons who implement access to user electronic information shall make reasonable records and logs of the steps taken to access the information. All implementation records shall be delivered to and preserved by the University Chief Information Officer.

Copies of the information accessed should be retained as needed to effectuate the purposes of the access.

The accessed information and the records and logs of the search shall be kept appropriately secure.

In all instances of access under this policy, records adequate to permit effective review as described in Part VI of this policy should be kept.

VI. Oversight Committee

This policy, its implementation, and instances of access under this policy shall be subject to review by an oversight committee to be constituted by the University, which shall include faculty and senior administrators. The oversight committee shall make recommendations to the President as to the implementation of the policy and possible amendments. The oversight committee shall also make periodic public reports on the implementation of this policy.

In carrying out its responsibilities, the oversight committee may review the records described in Part V of this policy, subject to redaction as necessary to protect individual users.

Exhibit 3

It's Your Yale

1607 Information Technology Appropriate Use Policy

PRINT (https://your.yale.edu/print/26531) EMAIL (https://your.yale.edu/printmail/26531)

Responsible Official: Chief Information Officer
Responsible Office: Information Technology Services
Effective Date: September 26, 2000
Revision Date: May 20, 2011

Policy Sections

Scope

This Policy applies to all Users of IT Systems, including but not limited to University students, faculty, and staff. It applies to the use of all IT Systems. These include systems, networks, and facilities administered by ITS, as well as those administered by individual schools, departments, University laboratories, and other University-based entities.

Use of IT Systems, even when carried out on a privately owned computer or other device that is not owned, managed, or maintained by Yale University, is governed by this Policy.

Policy Statement

The purpose of this Policy is to ensure an information technology infrastructure that promotes the basic missions of the University in teaching, learning, research, patient care, and administration. In particular, this Policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and superior performance of IT Systems;
- To ensure that use of IT Systems is consistent with the principles and values that govern use of

other University facilities and services;

- To ensure that IT Systems are used for their intended purposes; and
- To establish processes for addressing policy violations and sanctions for violators.

Reason for the Policy

Information technology ("IT") is used daily to create, access, examine, store, and distribute material in multiple media and formats. Information technology plays an integral part in the fulfillment of Yale University's research, education, clinical, administrative, and other roles. Users of Yale's IT resources have a responsibility not to abuse those resources and to respect the rights of the members of the community as well as the University itself. This Yale University IT Appropriate Use Policy (the "Policy" or "AUP") provides guidelines for the appropriate use of Yale's IT resources as well as for the University's access to information about and oversight of these resources.

University policies that govern freedom of expression and related matters in other contexts also govern electronic expression. This Policy addresses circumstances that are particular to the IT arena and is intended to augment but not to supersede other relevant University policies.

For statements of other applicable University policies, consult the Undergraduate Regulations, the Graduate School Program and Policies, the Faculty Handbook, and the Personnel Policies and Practices Manual, as well as policy manuals and statements issued by each individual graduate and professional school. The policies of Yale's Department of Information Technology Services ("ITS") govern the use of Yale IT Systems, and individual departments and schools at Yale may have specific IT policies that elaborate on ITS' basic policies.

Definitions

IT Systems: These are servers, personal computing devices, applications, printers, networks (virtual, wired, and wireless), online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by Yale University. For example, IT Systems include institutional and departmental information systems, faculty research systems, computer workstations and laptops, the University's campus network, and computer clusters.

User: A "User" is any person, whether authorized or not, who makes any use of any IT System from any location.

Systems Authority: While Yale University is the legal owner or operator of all IT Systems, it delegates oversight of particular systems to the head of a specific subdivision, department, or office of the University ("Systems Authority"), or to an individual faculty member, in the case of IT systems

purchased with research or other funds for which he or she is personally responsible.

Systems Administrator: Systems Authorities may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular IT resources.

Certifying Authority: This is the Systems Administrator or other University authority who certifies the appropriateness of an official University document for electronic publication in the course of University business.

Specific Authorization: This means documented permission provided by the applicable Systems Administrator.

Policy Sections

1607.1 Appropriate use of IT Systems

Although this Policy sets forth the general parameters of appropriate use of IT Systems, faculty, students, and staff should consult school or departmental governing policies for more detailed statements on permitted use for their various roles within the community. In the event of conflict between IT policies, this Appropriate Use Policy will prevail.

A. **Appropriate Use**

IT Systems may be used only for their authorized purposes – that is, to support the research, education, clinical, administrative, and other functions of Yale University. The particular purposes of any IT System as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the User. Appropriate use restrictions extend to Users connecting to Yale IT Systems with devices not owned by Yale.

B. **Authorization**

Users are entitled to access only those elements of IT Systems that are consistent with their Specific Authorization. Upon request by a Systems Administrator or other University authority, Users must produce valid University identification.

C. **Specific Proscriptions on Use**

The following categories of use are inappropriate and prohibited:

1. **Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others.** Users must not deny or interfere with or attempt to deny or interfere with service to other Users in any way. Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also

prohibited.

2. **Use that is inconsistent with Yale's non-profit status**.
The University is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of IT Systems for non-Yale purposes is generally prohibited, except if specifically authorized and permitted under University conflict-of-interest, outside employment, and other related policies. Prohibited commercial use does not include communications and exchange of data that furthers the University's educational, administrative, research, clinical, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization.

3. **Use that suggests University endorsement of any political candidate or ballot initiative.**
Users must refrain from using IT Systems for the purpose of lobbying that connotes University involvement, except for authorized lobbying through or in consultation with the University's Office of the General Counsel.

4. **Harassing or threatening use**. This category includes, for example, display of offensive, sexual material in the workplace and repeated unwelcome contacts with another.

5. **Use damaging the integrity of University IT Systems or non-Yale systems**. This category includes, but is not limited to, the following activities:
a) Attempts to defeat system security.
b) Unauthorized access or use. The University recognizes the importance of preserving the privacy of Users and data stored in IT systems. Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. For example, a non-Yale organization or individual may not use non-public IT Systems without specific authorization; Users are prohibited from accessing or attempting to access data on IT Systems that they are not authorized to access; Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System; and Users must not intercept or attempt to intercept or access data communications not intended for them.
c) Disguised or impersonated use. For example, a user ("user A") with access permission to another user's ("user B") email account must not send emails from that account without clearly indicating that the communication is sent from user A on behalf of user B.
d) Distributing computer viruses or malicious code.
e) Unauthorized modification or removal of data or equipment.
f) Use in violation of law. Illegal use of IT Systems – that is, use in violation of civil or criminal law at the federal, state, or local levels – is prohibited. Examples of such uses are: promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; and making bomb threat

6. Use in violation of law

   With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

7. Use in violation of University contracts.

   All use of IT Systems must be consistent with the University's contractual obligations, including limitations defined in software and other licensing agreements;

8. Use in violation of University policy

9. Use in violation of external data network policies

D. **Free Inquiry and Expression**

Users of IT Systems may exercise rights of free inquiry and expression consistent with the principles of the 1975 Report of the Committee on Freedom of Expression at Yale and the limits of the law.

E. **Personal Account Responsibility**

Users are responsible for maintaining the security of their own IT Systems accounts and passwords and may not share passwords without the authorization of the System Administrator. Passwords must conform with guidelines published at 1610 GD.01 Selecting Good Passwords (http://your.yale.edu/policies-procedures/guides/1610-gd01-selecting-good-passwords). Users are presumed to be responsible for any activity carried out under their IT Systems accounts or posted on their personal web pages.

F. **Encryption of Data**

A staff member may only encrypt data with the permission of his or her supervisor or as required by Yale policy. All Yale employees who use IT Systems to store, access, transmit or receive electronic protected health information must encrypt that information as explained in Procedure 1607 PR.01 (http://your.yale.edu/policies-procedures/procedures/1607-pr01-endorsed-encryption-implementation-procedure). Other Users are encouraged to encrypt data for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks, but they should do so using endorsed software and protocols (see Yale Procedure 1607 PR.01 (http://your.yale.edu/policies-procedures/procedures/1607-pr01-endorsed-encryption-implementation-procedure) Endorsed Encryption Implementation Procedure). Users who elect not to use endorsed encryption software and protocols on IT Systems are expected to decrypt information upon official, authorized request. (see

section 1607.2, "Conditions for University Access").

G. **Responsibility for Content**

Official University information may be published in a variety of electronic forms. The Certifying Authority under whose auspices the information is published is responsible for the content of the published document.

Users also are able to publish information on IT Systems or over Yale's networks. Neither Yale nor individual Systems Administrators can screen such privately published material nor can they ensure its accuracy or assume any responsibility for its content. The University will treat any electronic publication provided on or over IT Systems that lacks a Certifying Authority as the private speech of an individual User.

1607.2 Conditions for University Access

The University places a high value on privacy and recognizes its critical importance in an academic setting. There are nonetheless circumstances in which, following carefully prescribed processes, the University may determine that other considerations outweigh the value of a User's expectation of privacy and warrant University access to relevant IT Systems without the consent of the User. Those circumstances are discussed below, together with the procedural safeguards established to ensure access is gained only when appropriate.

A. **Conditions**

In accordance with state and federal law, the University may access all aspects of Yale IT Systems (including devices not owned by Yale but connected to Yale IT Systems) without the consent of the User, in the following circumstances:

1. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT Systems; or
2. When required by federal, state, or local law or administrative rules; or
3. When such access to IT Systems is required to carry out essential business functions of the University; or
4. When required to preserve public health and safety; or
5. When there are reasonable grounds to believe that a violation of law or a significant breach of University policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or
6. For Users who were members of the Yale faculty or staff: When the User's employment at Yale has ended and there is a legitimate business reason to access the User's IT Systems

B. Process

Consistent with the privacy interests of Users, University access without the consent of the User pursuant to 1607.2 A (1) through (5) will occur only with the approval of the Provost and cognizant Dean (for faculty users), the Vice President for Human Resources and Administration (for staff users), the Dean of Yale College or of one of the graduate or professional schools, as appropriate (for student users), or their respective delegates, except when emergency access is necessary to preserve the integrity of facilities or to preserve public health and safety. The University, through the Systems Administrators, will log all instances of access without consent pursuant to 1607.2 A (1) through (5). Systems Administrators will also log any emergency access within their control for subsequent review by the Provost, Vice President for Human Resources and Administration, dean, or other appropriate University authority. A User will be notified of University access to relevant IT Systems without consent pursuant to 1607.2 A (1) through (4). Depending on the circumstances, such notification will occur before, during, or after the access, at the University's discretion. In the case of a former staff member, access without consent pursuant to1607.2 A (6) must be approved by one of the former staff member's supervisors or their successors and no logging or notice is required. In the case of a former faculty member, access without consent pursuant to 1607.2 A (6) must be approved by the department chair or cognizant dean and no logging or notice is required.

C. User access deactivations

In addition to accessing IT Systems, the University, through the appropriate Systems Administrator, may deactivate a User's IT privileges, whether or not the User is suspected of any violation of this Policy, when necessary to preserve the integrity of facilities, user services, or data. The Systems Administrator will attempt to notify the User of any such action.

D. Use of security scanning systems

By attaching privately owned personal computers or other IT resources to the University's network, Users consent to University use of scanning programs for security purposes on those resources while attached to the network.

E. Logs

Most IT systems routinely log user actions in order to facilitate recovery from system malfunctions and for other management purposes. All Systems Administrators are required to establish and post policies and procedures concerning logging of User actions, including the extent of individually-identifiable data collection, data security, and data retention.

F. Encrypted material. Encrypted files, documents, and messages may be accessed by the University under the above guidelines. See 1607.1 - F, above.

1607.3 Enforcement Procedures

A. **Complaints of Alleged Violations**

An individual who believes that he or she has been harmed by an alleged violation of this Policy may file a complaint in accordance with established University Grievance Procedures for students, faculty, and staff (including, where relevant, those procedures for filing complaints of sexual harassment or of racial or ethnic harassment). The individual is also encouraged to report the alleged violation to the Systems Authority overseeing the facility most directly involved, or to the University Information Security Office, which must investigate the allegation and (if appropriate) refer the matter to University disciplinary and/or law enforcement authorities.

B. **Reporting Observed Violations**.

If an individual has observed or otherwise is aware of a violation of this Policy, but has not been harmed by the alleged violation, he or she may report any evidence to the Systems Authority overseeing the facility most directly involved, or to the University Information Security Office, which must investigate the allegation and (if appropriate) refer the matter to University disciplinary and/or law enforcement authorities.

C. **Disciplinary Procedures**

Alleged violations of this Policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the relevant policy documents. Staff members who are members of University-recognized bargaining units will be disciplined for violations of this Policy in accordance with the relevant disciplinary provisions set forth in the agreements covering their bargaining units.

Systems Administrators and the Information Security Office may participate in the disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. Moreover, at the direction of the appropriate disciplinary authority, Systems Administrators and the Information Security Office are authorized to investigate alleged violations.

D. **Penalties**

Individuals found to have violated this Policy may be subject to penalties provided for in other University policies dealing with the underlying conduct. Violators may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the Systems Administrator.

E. **Legal Liability for Unlawful Use**

In addition to University discipline, Users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System.

F. Appeals

Users found in violation of this Policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

1607.4 Policy Development

This Policy may be periodically reviewed and modified by the Provost of the University, who may consult with relevant University committees, faculty, students, and staff.

Related Resources

1607 PR.01 ENDORSED ENCRYPTION IMPLEMENTATION PROCEDURE (http://your.yale.edu/policies-procedures/procedures/1607-pr01-endorsed-encryption-implementation-procedure)

Contacts

University Access & Enforcement Provost of the University 203-432-4444

Information Technology Services University Chief Information Officer 203-432-3262

Information Security University Information Security Officer 203-432-1248

Exhibit 4

Search

Clinical Policies & FAQ

Search this Department...

Policies

1. Students may only participate in one clinic at a time.
2. Students may take a maximum of 16 clinical credits over their time at Harvard Law School. This does not include credits earned through the clinical course component.

Please review the HLS Handbook of Academic Policies[37] for more information on degree requirements and credit limitations. LL.M. students should consult with the LL.M. program office for clinical credit restrictions.

FAQs

BASIC QUESTIONS

Who can participate in a clinic?[38]

Do all clinics have a clinical course component?[39]

Are there any pre-requisites for clinics?[40]

If the semester ends and I want to keep working with a clinic, what options do I have?[41]

Do clinic grades count towards Latin Honors?[42]

Does my work in the clinic satisfy the HLS Pro Bono Graduation Requirement?[43]

REGISTRATION AND ADD/DROP

How and when do I register for clinics?[44]

How long does add/drop last for clinics?[45]

CLINICAL CREDITS AND WORK SCHEDULES

EXTERNSHIP CLINIC PLACEMENTS

PUBLIC SERVICE SUMMARY AND CLINICAL EVALUATIONS

CONFIDENTIALITY AND PROFESSIONAL CONDUCT

CLINICAL EMAIL SYSTEM

Who can participate in a clinic?

J.D. students in their 2L and 3L year as well as LL.M. students can participate in clinics.

Due to Massachusetts rules on representing clients in criminal proceedings, 2 clinics require students be in their 3L year: the Criminal Justice Institute and the ITA Prosecution Perspectives Clinic (Criminal Prosecution Clinic).

Some clinics have additional course requisites or require U.S. Citizenship for security clearance purposes.

- ✔ See Clinical Registration for J.D. students[62]
- ✔ See Clinical Application for LL.M. students[63]

Do all clinics have a clinical course component?

Yes. Most clinical courses are 2-credit seminars that meet once a week for 2 hours.

The majority of clinical courses are restricted to students who are currently enrolled in the associated clinic since the clinic and course are meant to be taken during the same semester. However, there are a few clinical courses that do not follow this model. Please check the clinic's description in the HLS Course Catalog[64] to see what the required clinical course component is.

Are there any pre-requisites for clinics?

Few clinics have pre-requisites, but if you are looking to do a clinic that includes criminal proceedings, Evidence or Trial Advocacy Workshop are most likely pre-requisites or co-requisites.

The clinic description in the HLS Course Catalog[65] will list any pre or co-requisites.

The Harvard Negotiation and Mediation Clinic requires that students have taken the Negotiation Workshop before they are eligible to enroll.

If the semester ends and I want to keep working with a clinic, what options do I have?

Students who have taken a clinic can arrange to continue their clinical work into a subsequent semester or another year by applying for an Advanced Clinical placement[66].

The application requires the approval of your direct clinical supervisor and the clinic's faculty director.

Advanced clinical students do not take an additional clinical course component.

Do clinic grades count towards Latin Honors?

Yes – grades earned through a clinic will count towards Latin Honors.

If a student receives permission by the Assistant Dean of Clinical and Pro Bono Programs to exceed the clinical credit maximum of 16 clinical credits, any credits earned above the 16 will not count towards Latin Honors. All independent clinical projects (and occasional Credit/Fail graded clinics) do not count towards Latin Honors.

Does my work in the clinic satisfy the HLS Pro Bono Graduation Requirement?

Almost all clinics satisfy the HLS Pro Bono Requirement. There are a handful of clinics that may have a mix of pro bono and non-pro bono projects.

You can read the Pro Bono Graduation Requirement[67] or contact us with specific questions.

How and when do I register for clinics?

J.D. students register for most clinics every year in late March or early April through a preferencing process in Helios.

Students register for the entire upcoming academic year – fall, winter, and spring semesters.

Some clinics are offered on a by-application basis. Students apply to these clinics according to the rules and deadlines stated in the clinics' course catalog description.

LL.M. students also participate in many of the same clinics as J.D. students but have their own clinical application process.
Please see the information here[68].

Once clinical registration preferencing results have been released, students are able to add and drop clinics through Helios.

Students who are on the wait-list for clinics will receive automated wait-list offers if and when space becomes available.

See Clinical Registration[69]

See By-Application Clinics

How long does add/drop last for clinics?

As soon as registration preferencing results are released, add/drop period opens for clinics.

Students may choose to drop from a clinic up until that clinic's drop deadline, which is stated in the clinic's course catalog description.

Students may also add themselves to clinics with open seats at any time up until the clinic's drop deadline.

Clinic waitlists tend to move significantly between the initial registration preferencing and the next academic year, especially for the spring semester of the upcoming year.

If I drop from a clinic, can I stay in the required clinical course?

If you were enrolled in the class as a direct result of your clinic enrollment (i.e. the class is either for clinical students only or you enrolled in the class under a reserved clinical seat) then you must also drop the class.

I received a clinic waitlist offer and cannot accept it – help!

There are a few reasons that you may not be able to accept the clinic waitlist offer.

- Check to make sure that you have enough room in your schedule for the clinical credits and the clinical course component credits. J.D. students may not enroll in more than 16 credits in both the fall and spring semesters (and may not exceed 3 credits during winter term).
- You may be enrolled in another clinic during that semester. Students may only take one clinic at a time, so if you are enrolled in a different clinic in the same semester as the waitlist offer, you will need to drop your current clinic enrollment before being able to accept the waitlist offer.
- You may have already taken the clinic. Students who have enrolled in a clinic once may not enroll again through Helios. Students interested in continuing their work with a clinic they have already participated in should apply through the Advanced Clinical program.

If you continue to have problems accepting your clinical waitlist offer, please contact us!

What if I want to drop a clinic after the clinic's drop deadline?

Clinics line up clients, cases, and projects well before the semester begins, and depend on their enrollment numbers to determine how many cases to take. Thus, clinics have add/drop deadlines that are always **earlier**

than the regular course add/drop deadlines. Dropping after the clinic's add/drop deadline results in a "Withdrawal" (WD) notation on your transcript.

How do clinical credits work?

In a clinic, you earn academic credits (clinical credits) for the work you complete. The majority of clinics allow you to elect 3, 4, or 5 clinical credits, although some clinics have a set number of clinical credits. Each clinical credit equals 4 hours of clinical work per week or 48 hours per semester.

Terms available	Clinical Credits	Hours of work per week	Hours of work per semester
Fall, Spring	2 clinical credits	8 hours/week	96 hours
Fall, Spring	3 clinical credits	12 hours/week	144 hours
Fall, Spring	4 clinical credits	16 hours/week	192 hours
Fall, Spring	5 clinical credits	20 hours/week	240 hours

Over winter term, students receive 2 clinical credits. Students must be in residence working full-time at their placements, from the first day of winter term through the last day of winter term.

How do I change the number of clinical credits I am enrolled for?

Students can change their clinical credits in Helios up until the clinic's drop deadline. Once the add/drop deadline has passed, students may request a change to their clinical credits by emailing Maggie Bay[71] in the Office of Clinical and Pro Bono Programs.

Each semester has a deadline, about a month into the semester, by which students must request any changes to their credit enrollment. More information about changing your clinical credits can be found here: https://hls.harvard.edu/dept/clinical/clinical-credits[72]

I noticed that clinics do not have set time-blocks. How is my clinical work schedule determined?

Once students have been assigned a direct clinical supervisor, they will work with that supervisor to establish a clinical work schedule that fits with the rest of their academic schedule. Some clinics may have more detailed requirements about when (and where) the clinical work must be done.

Do I have to make up clinical work for holidays or vacation weeks?

You are responsible for consistently working the required number of hours each week throughout the semester, with exceptions for certain holidays and spring break week. During these excused absences, which you should coordinate in advance with your placement supervisor, you are required to ensure that all casework is covered and that clients are aware of your absence. Any unplanned hours missed from your weekly schedule of clinical work must be made up within a reasonable period of time on a schedule developed in conjunction with your clinical supervisor.

What are the differences between an In-House clinical placement and an Externship clinical placement?

In-House clinics are located on-campus in Cambridge or Jamaica Plain neighborhood in Boston, and are staffed by HLS employees: Clinical Professors of Law, Lecturers on Law, Clinical Instructors, Clinical Fellows, and program administrators who teach students in the clinic and in the classroom.

Externship clinics have a slightly different format. Students enrolled in an externship clinic are placed at a variety of outside organizations that fall under the clinic's subject area. Your direct clinical supervisor is most likely a licensed attorney at the organization you are working for. The director of the externship clinic serves as the instructor for the clinical course component. Students engage in clinical work on-site at the organization they have been placed with.

The Office of Clinical and Pro Bono Programs coordinates placements for most externship clinics.

Does transportation time count toward my clinical hours if I have to travel to my clinical placement?

Travel time does not count towards your clinical hours requirement.

Where can I view the pro bono hours that I've earned though my clinical placement?

All your clinical placements will be listed in Helios in the "Public Service" section under "Your Public Service" menu option.

Pro bono hours for your clinical placement are automatically calculated based on the number of clinical credits that you completed.

The supervisor and/or listed on my clinical position is inaccurate – how do I edit the position to reflect the correct information?

If you notice an error in the information listed in your Public Service Summary in Helios, please contact us

so that we may correct the information.

Please **do not** complete the evaluation until the information listed is accurate!

How do I view student evaluations of past clinical placements?

Student evaluation of clinics are available in Helios in the "Public Service" section under the "Jobs Search" menu option. Once on the Jobs Search screen, you can choose to filter by "Clinic" and select the clinics you'd like to view.

Do I need to complete an evaluation for my clinical placement?

Yes. Our office collects these evaluations as a way to monitor and improve students' clinical experiences.

As the office that oversees the entire clinical program, we are always looking for student feedback about what works and what doesn't work, and where there may be opportunities for new ideas or programs.

We also collect these evaluations to provide future students candid information about the realities of clinical work, which can help them as they navigate the registration process and offer insights particular to the student experience.

What kind of guidelines do I need to follow as a student attorney?

In order for students to practice law, they must be practicing under the auspices of an existing clinic. You must not identify yourself as an attorney or give the impression to clients that you are an attorney, even though you have all the responsibilities and obligations of an attorney. Always advise clients and others that you are a law student. If someone mistakenly refers to you as an attorney or otherwise indicates that they think you are an attorney, you must clarify that you are a student.

The Massachusetts Rules of Professional Conduct[73] or the rules or codes of the particular jurisdiction of your placement apply to you. Please make sure that you are familiar with these rules and can access them during the semester.

When questions or problems arise, there are many resources available to you, including your supervising attorney and the Office of Clinical and Pro Bono Programs. Learn more at the Dean of Students[74] page.

Are there any confidentiality issues I should know about?

The majority of students enrolled in a clinical are working in a law office environment, practicing under a

special court rule. Because of this, you are bound by the same "attorney/client" confidentiality rules as staff at each placement site. While most clinical placements will address confidentiality issues with you, please feel free to raise any questions or concerns you may have with your supervisor.

We recommend the following as a starting point for dealing with client confidentiality:

- At all times, assure the client that all matters discussed relating to his or her legal problem and all written materials relative to the client or case are confidential. This also applies to potential clients you interview who are seeking legal advice.
- At the beginning of your clinical work, discuss any potential conflicts of interest with your supervisor, including any prior knowledge or legal work you may have accomplished on behalf of an opposing party.
- Do not refer to a client by name, provide identifying information or talk about details of the case in common areas of the office (reception area, hallway, elevators) where other clients or visitors may overhear you. This same rule applies when you are outside of the office (e.g., at a local restaurant), or when you're in a law school setting such as a class. Although we encourage the integration of clinical work into the classroom, you must never write a law school paper or exam, or provide your professor with case file documentation containing the client's name or other identifying information about the case or client.
- Handle case files carefully to avoid breaching client confidentiality. Whenever possible, case files and case-related documents should be kept in a filing cabinet, not on a desktop, where confidential information could be viewed by anyone walking by. Case files belong to the clinc and as such, all case/client related papers, files, emails, and electronic documents must be returned to the clinic by the end of the semester.

Do I need to use the clinical email system?

If you are doing clinic work or working in a Student Practice Organization, you must use the clinical e-mail account exclusively.

Students working at an externship and pro bono placement must adhere to the policies set forth by their organizations. Many organizations provide students with an email address to use for their work during the placement. If the placement does not provide this, students should discuss the existence of their clinical email account with their supervisor and should use this account.

Students should not use their personal email account or their regular HLS student account for externship or pro bono work.

The clinical email account has extra security measures in place to protect the confidentiality of the student, the supervisor, and the clients from inadvertent disclosure of confidential information. This email account should never be used for personal or other matters unrelated to clinical/pro bono work.

Links

1. https://hls.harvard.edu/dept/clinical/
2. https://hls.harvard.edu/dept/clinical/clinics/
3. https://hls.harvard.edu/dept/clinical/clinics/in-house-clinics/
4. https://hls.harvard.edu/dept/clinical/clinics/externship-clinics/
5. https://hls.harvard.edu/dept/clinical/clinics/advanced-clinical-program/
6. https://hls.harvard.edu/dept/clinical/clinics/independent-clinical-work-program/
7. https://hls.harvard.edu/dept/clinical/creating-a-placement/
8. https://hls.harvard.edu/dept/clinical/submitting-an-application/
9. https://hls.harvard.edu/dept/clinical/student-responsibilities/
10. https://hls.harvard.edu/dept/clinical/funding/
11. https://hls.harvard.edu/dept/clinical/funding-domestic/
12. https://hls.harvard.edu/dept/clinical/clinical-email-system-policy/
13. https://hls.harvard.edu/dept/clinical/funding-domestic/
14. https://hls.harvard.edu/dept/clinical/clinical-policies/
15. https://hls.harvard.edu/dept/clinical/clinical-registration-and-adddrop-deadlines/
16. https://hls.harvard.edu/dept/clinical/clinical-application-for-ll-m-students/
17. https://hls.harvard.edu/dept/clinical/clinical-credits/
18. https://hls.harvard.edu/dept/clinical/by-application-clinics/
19. https://hls.harvard.edu/dept/clinical/clinical-adddrop-deadlines/
20. https://hls.harvard.edu/dept/clinical/pro-bono-program/
21. https://hls.harvard.edu/dept/clinical/pro-bono-graduation-requirement-2/
22. https://hls.harvard.edu/dept/clinical/student-practice-organizations-spos/
23. https://hls.harvard.edu/dept/clinical/student-practice-organizations-spos/spo-officer-information/
24. https://hls.harvard.edu/dept/clinical/sign-up-and-apply-to-spos/
25. https://hls.harvard.edu/dept/clinical/student-pro-bono-opportunities/
26. https://hls.harvard.edu/dept/clinical/spring-break-pro-bono-trips/
27. https://hls.harvard.edu/dept/clinical/info-for-f-1-visa-j-d-students/
28. https://hls.harvard.edu/dept/clinical/student-forms/
29. https://hls.harvard.edu/dept/clinical/clinical-faculty-the-mentoring-advantage/
30. https://hls.harvard.edu/dept/clinical/for-attorneys-and-supervisors/
31. https://hls.harvard.edu/dept/clinical/for-attorneys-and-supervisors/supervising-students/
32. https://hls.harvard.edu/dept/clinical/for-attorneys-and-supervisors/attorney-and-supervisor-forms/
33. http://blogs.harvard.edu/clinicalprobono/
34. https://hls.harvard.edu/dept/clinical/newsletters/
35. https://hls.harvard.edu/dept/clinical/contact-us/
36. mailto:clinical@law.harvard.edu
37. /dept/academics/handbook/rules-relating-to-law-school-studies/
38. #faq-1-1
39. #faq-1-2

40. #faq-1-3
41. #faq-1-4
42. #faq-1-5
43. #faq-1-6
44. #faq-2-1
45. #faq-2-2
46. #faq-2-3
47. #faq-2-4
48. #faq-2-5
49. #faq-3-1
50. #faq-3-2
51. #faq-3-3
52. #faq-3-4
53. #faq-4-1
54. #faq-4-2
55. #faq-5-1
56. #faq-5-2
57. #faq-5-3
58. #faq-5-4
59. #faq-6-1
60. #faq-6-2
61. #faq-7-1
62. https://hls.harvard.edu/dept/clinical/clinical-registration-and-adddrop-deadlines/
63. https://hls.harvard.edu/dept/clinical/clinical-application-for-ll-m-students/
64. https://hls.harvard.edu/academics/curriculum/catalog/index.html
65. https://hls.harvard.edu/academics/curriculum/catalog/index.html
66. https://hls.harvard.edu/dept/clinical/clinics/advanced-clinical-program/
67. https://hls.harvard.edu/dept/clinical/pro-bono-graduation-requirement-2/
68. https://hls.harvard.edu/dept/clinical/clinical-application-for-ll-m-students/
69. https://hls.harvard.edu/dept/clinical/clinical-registration-and-adddrop-deadlines/
70. https://hls.harvard.edu/dept/clinical/by-application-clinics/
71. mailto:mbay@law.harvard.edu
72. https://hls.harvard.edu/dept/clinical/clinical-credits
73. http://www.mass.gov/obcbbo/rpcnet.htm
74. https://hls.harvard.edu/dept/dos/

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF VERMONT

JANET JENKINS, et al., Plaintiffs, v. KENNETH L. MILLER, et al., Defendants.	No. 2:12-cv-184-WKS

DECLARATION OF J. TYLER CLEMONS
IN SUPPORT OF PLAINTIFFS' REPLY IN SUPPORT OF THEIR MOTION TO COMPEL DEFENDANTS LIBERTY COUNSEL, INC., AND RENA LINDEVALDSEN TO COMPLY WITH PLAINTIFFS' FIRST REQUESTS FOR PRODUCTION

I, J. Tyler Clemons, declare under penalty of perjury that the following is true and correct:

1. My name is J. Tyler Clemons and I am counsel for Plaintiffs in the above-captioned action.

2. On November 7, 2018, Plaintiffs served a subpoena on non-party Liberty University. On June 18, 2019, Defendants Liberty Counsel and Rena Lindevaldsen served Plaintiffs with a document-by-document privilege log for 82 documents responsive to Plaintiffs' subpoena to Liberty University over which Defendants asserted the attorney–client privilege. A true and correct copy of this privilege log is attached to this motion as Exhibit 1.

3. I accessed Harvard University's "Policy on Access to Electronic Information" at http://hwpi.harvard.edu/files/provost/files/policy_on_access_to_electronic_information.pdf on September 23, 2019. A true and correct copy of that policy is attached as Exhibit 2 to this motion.

4. I accessed Yale University's "Information Technology Appropriate Use Policy" at https://your.yale.edu/policies-procedures/policies/1607-information-technology-appropriate-use-policy on September 23, 2019. A true and correct copy of that policy is attached as Exhibit 3 to this motion.

5. I accessed Harvard Law School's "Clinical Policies & FAQ" at https://hls.harvard.edu/dept/clinical/clinical-policies/#faq-7-1 on September 23, 2019. A true and correct of that website is attached as Exhibit 4 to this motion.

6. I make this Declaration on my own knowledge, information, and belief.

DATED at New Orleans in the Parish of Orleans and State of Louisiana this 23d day of September, 2019.

J. Tyler Clemons