



ADL Summer Associate Research Program 2020

Question 1: As large numbers of people turn to video-teleconferencing (VTC) platforms to stay connected in the wake of the COVID-19 crisis, reports of VTC hijacking (also called “[Zoombombing](#)”) are emerging nationwide. Virtual meetings are being disrupted by graphic, racist, antisemitic and/or threatening messages, and at times, perpetrators are intentionally targeting victims based on protected characteristics (i.e., to interfere with religious worship). Please identify and analyze viable civil causes of action in your jurisdiction (statutory, constitutional, contractual, common law tort, etc.) that could be used to hold “Zoombombers” accountable for their conduct. In addition, please consider possible theories of liability against Zoom for the actions of “Zoombombers” on the platform. Finally, please analyze whether there are any gaps in existing civil or criminal laws in your jurisdiction that should be filled in order to deter Zoombombing in the future.

Question 2: Like governments around the world, the United States is taking a multi-pronged approach to combat COVID-19. [Contact tracing](#) has been identified as a potential intervention method to break chains of transmission of infectious diseases, like COVID-19, for many years. As COVID-19 continues to spread at a rapid pace and traditional contact tracing methods require significant time and manpower, the United States is looking into digital contact tracing programs. For example, recently, Apple and Google announced a joint contact tracing program using Bluetooth technology to track coronavirus cases and potential exposure. What privacy and constitutional issues, if any, does digital contact tracing raise? What requirements, if any, could be proposed so that digital contact tracing would pass constitutional muster? What liability, if any, could governmental or private actors be subject to for a) collateral harms resulting from digital contact tracing, such as unintentionally outing members of the LGBTQ+ community, or b) if technological failings result in not performing contact tracing properly?

Question 3: The COVID-19 pandemic has upended religious life in America. Public health orders have temporarily closed large swaths of businesses and non-profits, including houses of worship. Many religious communities have adapted to this “new normal,” but others are challenging these orders in the courts. Many of the state stay-at-home orders effectively bar in-person religious worship. These have drawn dozens of lawsuits with mixed results, which have depended on the specifics of orders, as well as the judges evaluating them. Please provide a survey of the current legal landscape- directives, orders, bills, cases, etc.- in the United States and an analysis on the legality of directives and legal challenges in your jurisdiction.

Question 4: Under Missouri law, voters cannot vote by mail through an absentee ballot. There are exceptions to the law, including religious belief or practice. Six other states have similar rules. Recently, a group of [Rabbis wrote an open letter](#) encouraging Missourians to invoke the rule based on Jewish religious beliefs about preserving life. Furthermore, states like Texas do not allow absentee ballots based on religious belief or practice. However, it has a broad and robust religious freedom restoration act (“RFRA”). Research and analyze the following questions. For each of the seven states with a religious belief or practice exception to their absentee ballot law, would the state be required to provide an absentee ballot to a voter who invokes their sincerely religious beliefs or practices? In states having RFRA with restricted vote by mail laws, could a voter successfully invoke their sincerely held religious belief or practice to obtain an absentee ballot or otherwise vote by mail?

Question 5: [Section 230](#) of the Communications Decency Act (“CDA”) generally provides websites, blogs, and social networks that host speech with protection against a range of laws that might otherwise hold them legally responsible for what their users say and do. However, Section 230 does not protect tech companies from being held accountable for their own wrongful conduct (such as when tech platforms engage in unfair and deceptive trade practices, and/or publish original content). Please consider how state consumer protection or UDAP statutes might be used to hold platforms accountable when users repeatedly violate the platform’s terms of service, which often set user expectations (this hyperlinked [FTC complaint](#) may provide a launching point for



research). Please also consider what viable legal claims tech platforms might have against individuals who violate their terms and conditions, and what incentives tech platforms might have to bring these types of claims (this [article](#) re: a case pending in N.D. Cal. (3:2019cv03418) may provide a launching point for research). While you can briefly reference President Trump's [Executive Order](#) regarding Section 230, please focus on claims independent of the order.

Question 6: In February 2019, ADL released a survey related to the [American experience of Online Hate and Harassment](#). It revealed that online harassment is on the rise and many individuals are harassed in connection to their immutable characteristics. ADL is planning on releasing an updated survey this year. This report motivated ADL to engage in a legislative landscape analysis to better understand the criminal laws on the books (at the state and federal level) related to doxing, swatting, non-consensual distribution of intimate imagery (also sometimes referred to as non-consensual pornography), cyberstalking, cyberharassment and cyberstalking. It also motivated our launching of [Backspace Hate](#) (more on that below). ADL would like to learn more about the following to decrease online harassment: What administrative actions can be taken to increase protections for victims and targets of online hate and harassment? Are there any local ordinances in place to protect victims and targets of online hate and harassment? If so, how have they worked? If not, how might ADL work with municipalities to support victims and targets of internet-enabled abuse?

Question 7: Last year, ADL launched an initiative entitled “Backspace Hate” to support victims and targets of online hate and harassment by raising awareness and passing legislation to better hold perpetrators accountable for their actions online. ADL is particularly interested in strengthening laws with respect to [swatting](#) (the act of falsely reporting an emergency to someone’s home with the goal of having a police unit (usually a SWAT team) deployed to their residence) and [doxing](#) (the broadcasting of private or identifying information about an individual, group or organization with the intent that the information be used against the target for an unlawful purpose). In the meantime, however, we would like to support victims of both of these crimes through civil litigation. What viable causes of action might exist in your jurisdiction for victims of swatting / doxing (invasion of privacy, defamation, intentional infliction of emotional distress, etc.)? Is there any case law that would support these theories of liability? What possible defenses may be raised in response to these claims?

Question 8: Last year, ADL launched the first-of-its-kind [game survey](#) about online harassment and positive experiences in gaming. Looking at these digital environments that serve as digital social spaces in similar ways to social media platforms, the survey found an equal amount of harassment experienced by players in both text chat and voice chat in online games. At present, there are means to do content moderation in text chat, but these tools/techniques/policies do not currently exist for audio content moderation. ADL is working with the gaming industry on recommendations related to content moderation to keep users safe from hateful and harassing content by recommending [moderation tools for voice-based online communities](#). ADL is particularly interested in understanding the legal constraints related to [audio content moderation](#). To address this need, games and similar platforms may want to incorporate recording functionality within their content moderation processes. While there are already third-party applications that are able to record voice channels, such applications may pose privacy risks to users. On the other hand, if implemented within the platform, audio recording (and other features like video files, or audio files with metadata) largely require some type of automated system to listen in the voice channels at all times. What privacy concerns do these issues raise? Further, one-party consent recording is against the law in several states in the U.S. Would audio content moderation on platforms trigger wire-tapping laws? What if any additional legal and constitutional concerns are raised by audio content moderation on private platforms? What recommendations from a policy, legislative or administrative standpoint would you recommend for ADL to advocate regarding audio content moderation?