LEGAL AND ETHICAL ISSUES IN THE USE OF TELEPRESENCE ROBOTS: BEST PRACTICES AND TOOLKIT

Working Draft: March 27, 2015

We Robot 2015 Fourth Annual Conference on Robotics, Law & Policy
April 10 - 11, 2015
University of Washington School of Law

Chelsea Barabas
MS Student, MIT Comparative Media Studies

Christopher Bavitz
Clinical Professor of Law, Harvard Law School
Managing Director, Cyberlaw Clinic
Faculty Director, Berkman Center for Internet & Society

J. Nathan Matias
PhD Student, MIT Media Lab

Cecillia Xie
Harvard Law School (JD16)
Cyberlaw Clinic Student, Spring 2015

Jack Xu
Harvard Law School (JD15)
Cyberlaw Clinic Student, Spring 2015

Background and Acknowledgments

This paper is the product of an ongoing collaboration between Chelsea Barabas and J. Nathan Matias of the Massachusetts Institute of Technology and Harvard Law School's Cyberlaw Clinic, based at Harvard's Berkman Center for Internet & Society. Barabas, Matias, and the Clinic are in the process of creating an online toolkit designed to offer legal and ethical guidance to and best practices for users of telepresence robots. The work began in connection with The People's Bot project, launched by Barabas and Matias during a series of conferences and public events in the spring of 2014.

The authors extend special thanks to Microsoft Research, for providing WIFI to The People's Bot during the Association for Computing Machinery 2014 CHI Conference on Human Factors in Computing Systems in Toronto, Ontario; to the organizers of Theorizing the Web, for providing special access to The People's Bot; to the MIT Media Lab, for providing access to a pool of telepresence robots; to DoubleRobotics, for giving the authors early access to software for sharing robot time; to John Tang, for offering advice on robot training; to Andrés Monroy Hernández, for taking on the role of stand-in bot companion; and to Feola Odeyemi (Harvard Law School JD16), for his work as a fall 2014 Cyberlaw Clinic student helping to conduct research and create an outline that informed the development of the toolkit.

This paper is a work in progress. Information contained herein is based on general principles of law and is intended for information purposes only; the authors make no claim as to the comprehensiveness or accuracy of the information. It is not offered for the purpose of providing individualized legal advice. Use of this guide does not create an attorney-client or any other relationship between the user and the authors or the Cyberlaw Clinic.

Introduction

In 2014, Edward Snowden was present in Vancouver to attend the annual Technology, Entertainment, Design conference. Sort of. Since his historical leak of NSA surveillance documents, Snowden has been living in exile abroad in order to avoid prosecution from the U.S. government. Yet, in spite of severe restrictions on his mobility across borders, he was able to attend the high-profile TED event from an undisclosed location in Russia via robot, which enabled him to move around stage as he presented his views on privacy and surveillance to a captivated audience thousands of miles away.[1]

Snowden's appearance showed the power of robotic telepresence to extend opportunities to people who otherwise would not have access to high-profile events like TED. On the other hand, the Snowden bot also demonstrates the tendency of cutting edge technologies to extend the reach of only the most well-known, wealthy, and elite members of society. Many of the most common markets for robotic telepresence are workplaces, where executives and managers use them to extend their physical presence and view of workers or telecommuters use them to attend meetings.

Beyond their use by elite individuals, telepresence robots are increasingly being used to open access to social spaces for people who can't otherwise be present. In New York[2] and Texas[3], students with extreme allergies or immune deficiencies have attended class through telepresent robots. One Alaska school district used a fleet of fourteen telepresent robots for teachers to reach their students during harsh weather.[4]

Robotic telepresence is also being used to connect families across distances. For example, one study explored the potential for telepresent robots to mediate family care for people experiencing dementia[5]. Robotic telepresence has been used to offer remote access to museums, from early

---

[1] "Edward Snowden: Here's How we Take Back the Internet," TED2014 (Filmed March 2014), available at www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet (last visited March 15, 2015).

[2] Gillian Mohney, "Boy With Severe Allergies Attends School via Robot," ABC News (May 3, 2013), available at http://abcnews.go.com/blogs/health/2013/05/03/boy-with-severe-allergies-attends-school-via-robot/ (last visited March 15, 2015).

[3] "Student Lyndon Baty Attends School in Texas Via Vgo Robot," Huff Post Education (Posted February 4, 2011, Updated May 25, 2011), availalbe at http://www.huffingtonpost.com/2011/02/06/texas-student-lyndon-baty-vgo-robot_n_818884.html (last visited March 15, 2015).

[4] Lucija Millonig, "'Telepresence Robots' Connect Virtual Teachers With Classrooms," Education Week (February 3, 2014), available at http://blogs.edweek.org/edweek/DigitalEducation/2014/02/telepresence_robots_connect_virtual_teachers_with_classrooms.html (last visited March 15, 2015).

[5] Wendy Moyle, Cindy Jones, Marie Cooke, Siobhan O'Dwyer, Billy Sung, and Suzie Drummond, "Connecting the Person with Dementia and Family: A Feasibility Study of a Telepresence Robot," BMC Geriatrics (January 24, 2014), available at http://www.biomedcentral.com/1471-2318/14/7 (last visited March 15, 2015).

2001 research experiments by the Foundation of the Helenic World[6] to more widespread use by museums like the Tate,[7] the DeYoung,[8] and the National Museum in Australia.[9] One researcher on robotic telepresence, Kavita Krishnaswamy, has carried out extensive fieldwork for her PhD about telepresence in daily living by using systems herself, as someone with limited mobility due to spinal muscular atrophy.

The People's Bot

In 2014, Barabas and Matias developed The People's Bot to begin a conversation about future opportunities to use robotic telepresence for values of inclusion and public good -- broadening access, supporting public interest reporting, and funding access initiatives. The project proceeds from a belief that robotic telepresence can have much wider implications for access and inclusion in society.

Promotional image for The People's Bot, May 2014.

The People's Bot relates to Sam Gregory's idea of "co-presence for good" in human rights and disaster response.[10] Responders and activists are using video conferences to bring together diverse teams across barriers of geography, exclusion, and

---

[6] Maria Roussou, Panos Trahanias, George Giannoulis, George Kamarinos, Antonis Argyros, Dimitris Tsakiris, Pantelis Georgiadis, Wolfram Burgard, Dirk Haehnel, Armin Cremers, Dirk Schulz, Mark Moors, Elias Spirtounias, Mika Marianthi, Vassilis Savvaides, Alexandra Reitelman, Dimitrios Konstantios, Andromachi Katselaki, "Experiences from the Use of a Robotic Avatar in a Museum Setting," VAST '01 Proceedings of the 2001 Conference on Virtual Reality, Archeology, and Cultural Heritage (2001), available at http://dl.acm.org/citation.cfm?id=584993.585017&coll=DL&dl=ACM&CFID=475661211&CFTOKEN=56447112 (last visited March 15, 2015).

[7] Michelle Starr, "Explore Britain's Tate Museum After Dark via Robot," CNet (August 12, 2014), available at www.cnet.com/news/explore-britains-tate-museum-after-dark-via-robot/ (last visited March 15, 2015).

[8] Jon Kelvey, "A Quick Reminder that Technology Can Be Wonderful: Telepresence Robots Make it Possible for People with Disabilities to Visit Museums," Slate (July 22, 2014), available at http://www.slate.com/articles/technology/future_tense/2014/07/telepresence_robots_make_museums_accessible_to_everyone.html (last visited March 15, 2015).

[9] "Visiting the National Museum," Commonwealth Scientific and Industrial Research Organization, available at http://www.csiro.au/en/Research/DPF/Areas/Autonomous-systems/Telepresence/Museum-robot (last visited March 15, 2015).

[10] Institute for the Future, "Sam Gregory: Witness the Future," YouTube (November 21, 2013), available at https://www.youtube.com/watch?v=B9jlZkSe8JE (last visited March 15, 2015).

timezones. New technologies and modes like the MIT Media Lab's "unhangouts" are expanding tools available for fast collaboration and conversation across distance.[11] The People's Bot also draws upon work done by the Institute for Applied Autonomy, which created the idea of "contestational robots" that are used to introduce speech into areas where speech has been restricted.[12]

Leon Neyfakh of the Boston Globe reports on the CHI2014 session on robotic telepresence. Photo by Quentin Roy for the People's Bot.

Building from this work, Barabas and Matias used The People's Bot to provide access to high profile academic forums and conferences for people who otherwise would not be able to participate, experimenting with three different models for allocating access for the public good. Over the course of several weeks, they enabled eight individuals from three different countries to attend via telepresence one of three high-profile academic events: an exclusive meeting at the MIT Media Lab (during which the Lab's most recent projects are showcased to a broader audience), the Theorizing the Web Conference in New York, and the Computer Human Interaction (CHI) Conference in Toronto. This was done by creating a platform in which people could apply for the following opportunities:

- **Scholarships:** for high school, college, graduate students who are unable to attend the conference due to prohibitive cost of travelling and paying for the event;

- **Journalism Fellowships:** for bloggers and citizen media who are committed to sharing their experience with a broader audience; and

- **Auctions:** for anyone else interested in bidding for thirty minutes of telepresent roaming time.[13]

To use the DoubleRobotics telepresent robot, the owners of the robot first connect the robot to a server at DoubleRobotics through an iPad that also serves as a video interface. After using their

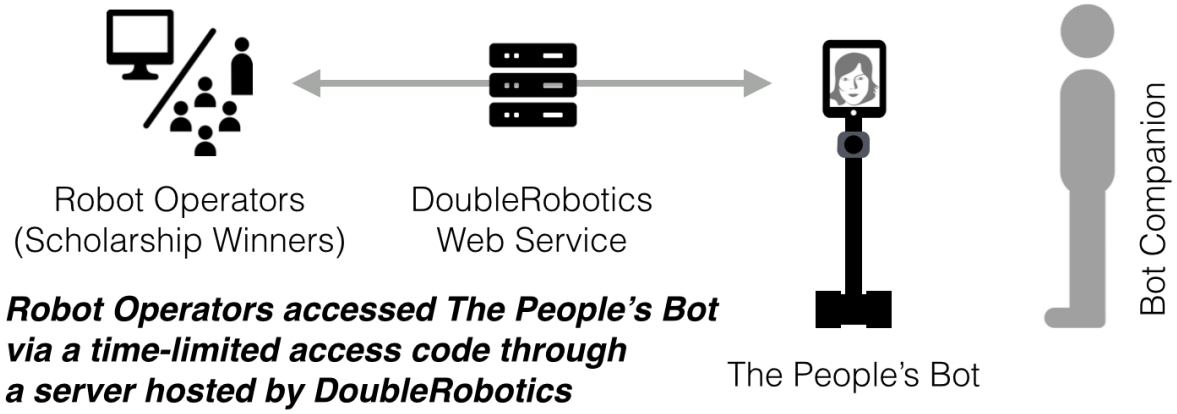
---

[11] Unhangout, available at https://unhangout.media.mit.edu (last visited March 15, 2015).

[12] Institute for Applied Autonomy, available at http://www.appliedautonomy.com/projects.html (last visited March 15, 2015).

[13] Barabas and Matias committed to donate proceeds from eBay auctions to the CHI student travel fund.

own login and password to confirm access, the owners of the robot then generate a time-limited, single-use access code and send it to the person who will be operating the bot for that period (the scholarship students or journalists). Upon logging in to the DoubleRobotics website, the operator is able to view streaming video from the robot, control its movement, control its height, park it, and also reply to anyone who speaks to the robot. At all times, the People's Bot team provided a "bot companion" who could restore the quality of the connection, guide the operator if needed, and offer social cues to event participants.



creative commons images licensed CC BY 3.0:
Face image by Jule Steffen & Matthias Schmidt. Server image by Hans Paul Mösl Junior. Person image by Irene Hoffman

Upon receiving a scholarship or fellowship, each operator was given a forty-five minute bot training session, which included an opportunity to view themselves in a mirror, navigate a physical space, speak with a person, attract a person's attention, and cope with broken connections from their computer to the DoubleRobotics web service or the robot's own Internet connection. Protocols were also established for establishing alternative communication with the bot companion at moments of broken connectivity or social confusion.

To support telepresent participation in an event, The Peoples Bot's designated bot companion flew to the city in question, checked in the robot as an attendee, and set up a charging station in a secure location at the event. The companion then unpacked and assembled the bot, tested it, and generated the time-limited access codes for each session, coordinating with the operators on the time and location of their participation. In between uses, the bot companion ensured that the robot was charged and that it was already in the predetermined location agreed with the operator.

Some operators preferred to participate between formal sessions, roaming the hallways for conversations. Others preferred to attend and write about talks. One journalist attended a session, set up interviews with attendees, and found a quiet corner at the conference to carry out interviews.[14]

[14] Neyfakh, Leon. "My Day as a Robot," Boston Globe Ideas (May 11, 2014), available at http://www.bostonglobe.com/ideas/2014/05/10/day-robot/6UAMgmUFn0mZhoMS8vy0GK/story.html (last visited March 24, 2015).

In addition to offering new models for telepresence in the public interest, The People's Bot was an exploration of the legal issues arising from the use of telepresent robots in public and closed events for learning, conversation, and media production. This paper and the larger planned toolkit address some of the key legal considerations one should take into account when deploying telepresent robots for increased access and opportunity in the general population.

Legal Issues and Framework

The use of telepresence robots in any of the settings described herein raises some legal and ethical concerns. Those concerns underscore the developing nature of robot-human interactions. Maximizing the utility of telepresence robots for good cannot come at the expense of honoring social norms and applicable laws and regulations. The toolkit in development endeavors to address fundamental considerations that should be taken into account when operating or permitting others to operate telepresence robots. It focuses on telepresence in the workplace, school, and broader public or quasi-public (e.g., conference) settings.

Definitional Considerations – What is Telepresence?

Telepresence robots provide users with the ability to sense and interact with remote environments, leading to an overall sense of extended agency in that environment. Unlike other forms of remote audiovisual interaction (such as videoconferencing), telepresence provides users with a greater ability to move in that environment and direct what the user can or cannot see.

A telepresence robot emulates how a human body might function in a remote environment, as if the person operating the robot were actually there. Telepresence robots are often designed to mimic the human body and frequently have roughly the same height or size.[15] The goal of telepresence is to provide a sense of extended agency or mirror the experience of otherwise being in a remote location. Telepresence robots may be modeled after human forms, so other observers will interact with a robot by adopting similar kinds of social norms as if the robot were a human.

Legal Considerations

Telepresence Use Case Study #1 – The Workplace

> *Hypothetical Fact Scenario (Workplace 1): Andy is a manager at a media company, who has to often travel across the country for work. He uses a telepresence robot in the office on days when he is out of the office, to attend meetings and otherwise communicate with co-workers. Occasionally, Andy's bot engages in sensitive or private conversations with co-workers about their business or personal lives. Andy is also called upon to approve business deals and sometimes to finalize and sign contracts at meetings while using a bot.*

[15] *See, e.g.*, Munjal Desai, Katherine M. Tsui & Holly A. Yanco, Essential Features of Telepresence Robots, Robotics Lab, http://robotics.cs.uml.edu/fileadmin/content/publications/2011/Essential_Features_of_Telepresence_Robots.pdf (last visited Mar. 25, 2015).

Many of the key underlying legal and ethical concerns that arise from the use of telepresence robots (and, thus, that run throughout this paper) are concerns about privacy. By virtue of their ability to sense (i.e., see and hear) remotely and transmit information about a given physical setting to a faraway user, telepresence robots necessarily raise concerns about surveillance and the expectations of those with whom the robots interact about the scope and nature of those interactions. Such concerns may be particularly acute in the workplace given commercial sensitivities around materials discussed or shared in office settings.

In the United States, federal law prohibits the interception of or eavesdropping on electronic communications (the Wiretap Act),[16] as well as accessing stored electronic communications without authorization (the Stored Communications Act).[17] The Stored Communications Act has been used against former employees who access their prior employer's computer systems.[18] The Wiretap Act could also potentially be used to punish former employees who intercept communications by their prior employer's systems, and courts have noted that "the intersection of the Wiretap Act… and the Stored Communications Act… is a complex, often convoluted, area of the law."[19]

Thus, accessing a telepresence robot while it is attending a meeting might be a violation of the Wiretap Act. Accessing stored video streams that the telepresence robot has cached, saved, or archived might violate the Stored Communications Act. The network that is accessed does not necessarily have to be encrypted in order for the access to be a violation of the Wiretap Act or the Stored Communications Act.[20] Violations of either statute may be punishable by civil damages and/or imprisonment.[21]

Another privacy concern that may arise in the workplace context involves a situation where an employee using the telepresence robot to remotely participate in workplace events violates her co-workers' expectations about privacy by listening in on conversations, observing activities, and/or sharing with third-parties information about those conversations and activities that that those co-workers did not reasonable expect to be seen or heard. Whether an invasion of privacy occurred may hinge on state privacy protections, which can include state constitutional provisions governing privacy and state statutes (such as wiretap laws that dictate whether a party

[16] 18 U.S.C.A. § 2511(1)(a) (West 2015).

[17] 18 U.S.C.A. § 2701(a) (West 2015).

[18] *Cyber Attacks*, S.C. Law. 20, 24 (Jan./Feb. 2002).

[19] United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998).

[20] *See* In re Google Inc. St. View Elec. Commc'ns Litig., 794 F.Supp. 2d 1067, 1084 (N.D. Cal. 2011) (finding that "merely pleading that a network is unencrypted does not render that network readily accessible to the general public and serve to remove the intentional interception of electronic communications from that network from liability under the ECPA").

[21] 18 U.S.C.A. § 2511(4)(a); 18 U.S.C.A. § 2701(b).

is a one-party or two-party consent state). In one California case, for example, a court looked at whether conduct constituted an "egregious breach of social norms," finding that information collected during the course of "routine commercial behavior" did not constitute such a breach.[22] Conversely, another court in Missouri found that intentionally intercepting a spouse's electronic communications in the marital home was an invasion of privacy.[23]

Whether Andy invaded a co-worker's privacy, then, may depend on what information was shared and how. Notice and/or permission are keys, legally and ethically, to responsible use of a telepresence robot. Andy should probably refrain from recording others without permission while using the bot. State privacy laws may impose additional constraints on what Andy can do with the bot, as notice and consent requirements differ from state to state.

> *Hypothetical Fact Scenario (Workplace 2): Andy often meets with clients to negotiate sales agreements that culminate in oral contracts. By using telepresent robots to conduct such meetings, Andy is able to not only save on time, energy, and travel costs, but also to manage a larger and more complex network of clients across remote parts of the country.*

It is generally good practice to put contracts in writing to minimize ambiguity. Nevertheless, as is the case with Andy, many businesspersons deal with each other using a traditional handshake across a table. When there is sufficient evidence of oral contracts, such as in the form of witnesses or video recordings, oral contracts may be enforceable. This was demonstrated in *Texaco vs. Pennzoil* where the court found that selling Getty Oil to Pennzoil in a handshake deal constituted a binding oral contract under New York law.[24]

There is a presumption against enforceability for deals of larger sizes and longer durations under the Statute of Frauds, and jurisdictions differ in the circumstances that require agreements to be in writing.[25] But, such presumptions can be defeated if a plaintiff can demonstrate a party partially performed the terms of the contract or relied on the terms and suffered as a result of such reliance.[26]

---

[22] In re iPhone Application Litig., 844 F.Supp. 2d 1040, 1063 (N.D. Ca. 2012) (disclosure to third parties of unique device identifier numbers, personal data, and geolocation information from iDevices was "routine commercial behavior"). *See also* Opperman v. Path, Inc., No. 13-CV-00453-JST, 2014 WL 1973378, at *27 (N.D. Cal. May 14, 2014) (copying someone's address books could be an egregious breach of social norms so as to justify a claim of invasion of privacy).

[23] Kempf v. Kempf, 868 F.2d 970, 972 (8th Cir. 1989).

[24] Texaco, Inc. v. Pennzoil, Co., 729 S.W.2d 768, 817 (Tex. App. 1987), writ refused NRE (Nov. 2, 1987) disapproved of by Durbin v. Dal-Briar Corp., 871 S.W.2d 263 (Tex. App. 1994) (court supported jury finding that a contract existed when parties expressed their intent to contract orally even though they had not yet signed the written document).

[25] *See* U.C.C. § 2-201(1) (1977).

[26] *See* U.C.C. § 2-201(3) (1977).

The use of telepresence robots adds a further dimension to the consummation of both oral and written contracts in commercial or workplace settings in a couple of important ways:

- First, telepresence may mask non-verbal cues, or render some of them impracticable. Telepresence may not fully convey a party's tone of voice, facial expression, body language, and/or gesture that can contain contextual information important for the interpretation of a contract's terms.

- In addition, negotiations via telepresence are typically not concluded with a physical handshake to demonstrate a meeting of the minds. This fact may make some courts more unwilling to enforce oral contracts made via telepresence.

In another light, telepresence technology can make it very convenient to record oral contract formation. Having an embedded camera record meetings may prove to be more socially acceptable (perhaps by virtue of being less physically intrusive) than using a standalone camera and might therefore make video records of oral contracts more commonplace. Such video records – again, assuming appropriate notice has been given to and/or permission obtained from all participants – could serve as evidence of the existence or terms of an agreement.

Businesses obviously must be mindful, in establishing practices around use of telepresence in the workplace, about business sensitivities relating to confidentiality of recorded information. They should coordinate closely with counsel around records retention obligations if such recordings are maintained in the general course of business.

Telepresence Use Case Study #2 – School or Other Educational Setting

> *Hypothetical Fact Scenario (School 1): Andy's son, Barry, also uses a telepresence robot. Barry uses the bot to attend school when his serious allergies prevent him from physically attending. One day, Barry accidentally backs the bot into a classmate, Ben. Ben gets angry and turns around, striking the bot.*

Using telepresence robots in the school setting opens up the possibility of potentially inappropriate contact between a child and the robot (or robot operator). Inappropriate contact is legally recognized as a component of the tort of battery, when an actor acts with the intention to cause harmful or offensive contact with the other and either directly or indirectly succeeds in making the offensive contact.[27]

What constitutes "offensive contact" is extremely broad, however, and does not require that one's actual body be disturbed.[28] "Unpermitted and intentional contacts with anything so

---

[27] Restatement (Second) of Torts § 18 (1965).

[28] *Id.*, cmt. c.

connected with the body as to be customarily regarded as part of the other's personality that he can accomplish his purpose of offending the other by some contact with it" can be seen as offensive contact for the purposes of battery.[29]

At least one commentator has suggested that, if a student were to hit the telepresence robot, the student has potentially committed battery on the robot end-user, as the robot is operating as an extension of the end-user's personality.[30] What is considered offensive contact, however, hinges upon violation of "a reasonable sense of personal dignity." Thus, an individual touching the robot in an attempt to get the robot's attention may not qualify as offensive contact, whereas kissing the robot or striking the robot may "offend the ordinary person" and qualify as offensive contact.[31]

Conversely, a robot user can commit physical torts on nearby humans. Although not many disputes of this type have been documented, there was a negligence lawsuit filed after a man died after an operation using the da Vinci surgical robot system.[32] The case was settled out of court, so no precedent was made to govern future liability issues that may arise from end-users intentionally or accidentally causing physical harm to others via robotic telepresence.[33] Nevertheless, the ability to commit torts through contact with the robot suggests that liability logically could flow in the other direction. Robot users should be careful to not harm bystanders – intentionally or negligently – with their robots. Those enabling access to robots, too, would be well-served by:

a. establishing training protocols to ensure robot operators are well-positioned to operate robots responsibly; and

b. attempting to mitigate, through contractual representations and indemnification obligations, the risk of liability by putting it, to the maximum extent possible, on the robot operator herself.

Currently, telepresent robots cost thousands of dollars for the typical consumer. Because they often operate in remote environments, where pilots do not have direct physical contact with the robot, property theft may be of concern. This is particularly true if a bot is operating in a public space, without on-site supervision.

---

[29] *Id.*

[30] *See* Neal Hoffman, *Battery 2.0: Upgrading Offensive Contact Battery to the Digital Age*, 1 Case W. Reserve J.L. Tech. & Internet 61, 71-72 (2010) (positing that plaintiffs can argue that an object is emotionally and psychologically connected enough with his person so that attacks on the object are attacks on the person).

[31] Restatement (Second) of Torts § 19, cmt. a.

[32] Joshua B. Good, *Lawsuit Targets Doctor's Training*, The Tampa Tribune (Dec. 17, 2003), at Metro 1, *available at* http://yerrid.com/verdict61.cfm.

[33] Jessica S. Allain, *From Jeopardy! To Jaundice: The Medical Liability Implications of Dr. Watson and Other Artificial Intelligence Systems*, 73 La. L. Rev. 1049, 1056 (2013).

The property tort of conversion may also be relevant when it comes to telepresent robots. For example, although one might not ordinarily be liable for any wrongdoing if they simply turn off someone's laptop, turning off another person's telepresent robot would deprive the pilot of control over the robot and could leave the bot vulnerable to theft. The person who interfered with the operation of the robot may therefore be partially liable for the lost property.

The authors are aware of no current caselaw that directly addresses the extent of someone's liability when she interferes with the operations of a telepresent robot, but bystanders should be aware that the same kinds of interference with traditional electronic equipment might amount more damaging consequences when they interfere with telepresence robots. It may also be in pilots' interests to use notices on their robots to warn bystanders about interference.

> *Hypothetical Fact Scenario (School 2): Barry uses his robot to record lessons in class, so that he can later review them. During the lessons, other students are sometimes recorded, as well as their questions or answers to the teacher.*

When Barry's bot records other students in the classroom, student privacy is a concern. Such recordings could constitute "education records" within the meaning of the Federal Educational Rights and Privacy Act (FERPA),[34] especially because the recordings make the students personally identifiable if their faces and voices are seen and heard. If the school maintains collection of Barry's recordings, the school may have to get written parental consent from the parents of the children identifiable in the recordings.[35] The school cannot generally disclose the recording to third-parties without obtaining written parental consent first.[36] If Barry keeps the recordings himself, he may be subject to general state privacy laws regarding recording conversations with others. Barry should make sure to get permissions from the school, the teacher, and his classmates (via parents) before recording classes with his bot.

Telepresence Use Case Study #3 – Public or Quasi-Public Setting (E.g., Conference)

> *Hypothetical Fact Scenario (Conference 1): Charlie wants to attend a robotics conference in San Francisco. Unfortunately, he lives in London. The travel costs are prohibitively expensive and prevent him from attending in person. He decides to borrow a telepresent robot from his cousin who works in San Francisco and register the robot as an attendee for the event. Having successfully registered for the event, Charlie posts the news on his social media profile and finds out that many of his friends would like to attend, too. He realizes there is value-creating potential with the use of his robot. He thinks of letting his friends use his robot during various time periods to attend particular talks at the conference and also creating a live feed to be streamed online using his robot's camera.*

[34] 20 U.S.C.A. § 1232g (West 2015).

[35] 20 U.S.C.A. § 1232g(a)(1)(A).

[36] 20 U.S.C.A. § 1232(g)(b)(1).

Depending on the types of events that Charlie attends, he may run into legal concerns around copyright infringement. Unauthorized public performances and/or transmissions of copyrighted works may violate a copyright owner's rights under the United States Copyright Act.[37] Using a robot to observe a talk at a conference and transmit or perform the substance of that talk – including any copyrighted material therein – may require licenses from relevant copyright holders.

Some uses of copyrighted content via a telepresence robot may qualify as fair uses. Under the Copyright Act, evaluating fair use involves balancing many factors, including the purpose and character of the use (e.g., whether the use is of a commercial nature or nonprofit educational purpose), the nature of the work, the amount and substantiality of the portion used in relation to the copyrighted work as a whole, and the effect of the use upon the potential market for or value of the copyrighted work.[38] If Charlie is intending to make money from leasing out his robot or with his live stream, the commercial nature of the operation might weigh against him in a fair use evaluation.

In addition, whether or not they fully appreciate it, conference attendees may be governed by contractual terms that dictate limitations on their rights at conference events and impose liability in the event such terms are breached. Charlie may wish to review those terms and, ultimately, check with event organizers before lending his robot to be used by others or streaming conference sessions. Potential options for the organizers might include:

a. granting Charlie permission, subject to a requirement that he clearly message to other attendees what the bot is doing; and/or

b. allowing for a second tier of access, beyond that granted to regular paying conference attendees, for robot operators who attend with the intention of permitting third-party access to conference events.

Again, conveying information to and managing expectations of all involved in human-robot interactions is key to minimizing legal liability.

> *Hypothetical Fact Scenario (Conference 2): Charlie agrees to let his friend, Chris, use the robot during the Artificial Intelligence panel, for a fee. The fee goes part of the way towards paying for the attendance fee that Charlie paid for the entire conference. Before Chris's allotted access of the robot starts, Chris's wife, Charlotte, hacks into the robot to access the video stream of the conference. Charlotte learned about the robot from Chris and decided to access the robot without paying or talking to Charlie. After the Artificial Intelligence panel ends, Chris retains access to the robot instead of logging off, in order to view the remainder of the conference without paying for the related fees.*

[37] 17 U.S.C. § 106.

[38] 17 U.S.C. § 107.

Conferences can create a wealth of electronic information from the panels, events, and discussions that occur. Chris and Charlotte, by accessing the robot without paying Charlie or the conference organizers for the different events they view, have potentially violated the Computer Fraud and Abuse Act (CFAA).[39] The CFAA has been "instrumental in prosecuting [individuals] for damages to and theft of electronic databases and information."[40]

The CFAA encompasses both those who "access[] a computer without any permission at all" (here, Charlotte) and those who have "permission to access the computer, but access[] information on the computer that the person is not entitled to access" (here, Chris).[41] Although the CFAA is primarily a criminal statute,[42] it has also been used to impose civil liability for the theft of electronic information.[43]

If Charlie or the conference organizers prove that Chris and Charlotte's access created economic damages for them, Chris and Charlotte can be prosecuted criminally or sued civilly. Thus, users sharing a robot to attend a paid conference should take care to not access a robot beyond what was agreed upon and paid for.

> *Hypothetical Fact Scenario (Conference 3): The organizers of the conference discover that a hacker accessed Charlie's robot during the conference and obtained valuable information disclosed during certain sessions. They further discover that the hacker accessed Charlie's robot, because Charlie did not set up any security systems that would make it difficult for others to access his robot.*

Charlie has potentially opened himself up to a lawsuit from the conference organizers. The best practice for Charlie may be to:

a. encrypt data from telepresence robots so that he cannot be seen as negligently exposing valuable information to security breaches; and/or

b. contractually establish the level of data security that he needs to provide.

Conclusion

The widespread use of telepresence robots in all manner of personal and business situations has the potential to radically expand access to information and facilitate human interactions across the globe. Careful attention to legal concerns at all stages of the process of using and

[39] 18 U.S.C.A. § 1030 (West 2015).

[40] *Cyber Attacks*, *supra* note 18, at 23.

[41] In re iPhone Application Litig., 844 F.Supp. 2d 1040, 1065 (N.D. Cal. 2012).

[42] *Id.*

[43] *Cyber Attacks*, *supra* note 18, at 23.

implementing use-programs that involve telepresence robots can ensure maximum value with minimal risk and disruption.

APPENDIX:
LEGAL ISSUES AND LEGAL GUIDE ROADMAP

Torts (General)

- Types of injuries
    - Physical torts
    - Property theft
- Damage to whom or what
    - Responsibility to people
    - Responsibility to pets
    - Responsibility to objects / property
- Potentially responsible parties
    - Responsibilities of the bot operator
    - Responsibilities of the bot companion
    - Responsibilities of the person in charge of the physical location where the bot is operating
    - Responsibilities of the manufacturer (e.g., product liability)

Privacy

- Wiretap Act (18 USC §§ 2510-2522)
    - Does not apply if communication is accessible to the general public, so would depend on the scope of the telepresence robot's feed.
    - Consider networks' and manufacturers' ability to copy or intercept robot users' data
    - "Electronic communications" and "interception" are interpreted broadly, and the transit-storage dichotomy is decreasingly relevant in the digital age
- Stored Communications Act (18 USC §§ 2701-2710)
    - May implicate accessing of recordings from the bot that are then stored
    - Users should make sure they are authorized to access stored data from the bot.
    - Has been interpreted to apply only to electronics communication service providers (e.g., Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998))
- Service provider exceptions of different scopes are in both Wiretap Act and SCA
    - Overlapping statutes, but claimants can bring actions under either
- Electronic Communications Privacy Act (ECPA) ties in heavily with societal "reasonable expectation of privacy"

- See Kyllo v. United States, 533 U.S. 27, 43 (2001) (Stevens, J., dissenting); Richard A. Posner, The Uncertain Protection of Privacy by the Supreme Court, 1979 Sup. Ct. Rev. 173, 188

- Law enforcement
  - Law enforcement may be able to access recordings
  - Who owns the recordings?
    - Does the owner of a recording have an obligation to those in the recording or to those who commissioned the recording to not turn it over to law enforcement?
    - Relevance of the third-party doctrine?
  - State law protections can be higher than Fourth Amendment (See, e.g., State v. Reid, 194 N.J. 386, 396-97 (N.J. 2008))
- State laws
  - Some states have broader protections than ECPA
    - State law may have different consent standards for recording conversations
  - State wiretap laws can impose requirements on those recording conversations around notice and consent
    - See, e.g., Mass. Gen. Laws ch. 272, § 99.

Cyber Security

- 18 USC § 1030, Computer Fraud and Abuse Act
  - Two situations are implicated:
    - Unauthorized individual hacks into the telepresence robot's stream (i.e., access without authorization)
    - Authorized individual continues access to bot after allotted time (i.e., access exceeding authorization)
  - CFAA is primarily a criminal statute, and actual economic damage needs to be shown (e.g., retention of personal information is not enough to show that economic damages under the CFAA occurred)
  - Bot operators and authorized users at the time unlikely to be held liable for unauthorized access or exceeding access by others
- Negligence/breach of contract for data breaches by third-party hackers
  - Consider standing issues for potential claimants

Intellectual Property

- Direct infringement

- Copyright owners have may rights over the performance and display of their works (depending on type of work)
- Definitions
  - Copyright Act § 101 – to "perform" a work means to recite, render, play, dance, or act it, either directly or by means of any device or process or, in the case of a motion picture or other audiovisual work, to show its images in any sequence or to make the sounds accompanying it audible
  - Copyright Act § 101 – to "display" a work means to show a copy of it, either directly or by means of a film, slide, television image, or any other device or process or, in the case of a motion picture or other audiovisual work, to show individual images nonsequentially
  - Copyright Act § 101 – to perform or display a work "publicly" means--
    - (1) to perform or display it at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered; or
    - (2) to transmit or otherwise communicate a performance or display of the work to a place specified by clause (1) or to the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times.

- Secondary liability
  - Contributory infringement
    - Direct infringement
    - Knowledge (actual or constructive) by the defendant
    - Material contribution
  - Vicarious infringement
    - Direct infringement
    - Financial interest in the infringement
    - Right and ability to supervise the direct infringer
  - Statutory safe harbors
    - ISP, 17 U.S.C. § 512
      - Service provider is defined as an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.
      - Requirements

    - Transmission of the material initiated by or at the direction of a person other than the service provider
    - Transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider
    - Service provider does not select the recipients of the material except as an automatic response to the request of another person
    - No copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections
    - Material is transmitted through the system or network without modification of its content
- Fair Use
    - Copyright Act § 107

Contracts

- Oral contracts
    - Scenarios:
        - Oral contract made between two people piloting two telepresence robots
        - Oral contract made between two people where one is communicating via a telepresence robot
    - Questions:
        - When is video evidence of an oral contract admissible in court?
        - Does it matter whether both parties consented to be filmed in the context of reaching an agreement?
        - Is consent required for a pilot to take video in the context of creating an oral contract?
        - How are oral contracts different from written contracts?
        - What if the oral contract is recorded on video?
    - Six requirements of a contract
        - Offer
        - Acceptance

        - Mutuality of obligation
        - Consideration
        - Competent parties
        - Lawful subject matter
    - Oral contracts vs. written contracts
        - Plaintiff holds the burden to prove the existence and the terms of an oral contracts by a preponderance of the evidence
        - Time to sue for breach of an oral contract under the Statute of Frauds is shorter (e.g. in California, it is two years for oral contracts but four for written)
        - Some contracts must be in writing
    - Validity of an oral contract
        - Testimony of witnesses, including video
        - Course of conduct
        - Credibility of individual parties
    - Parol Evidence Rule
- Video contracts
    - How is video data interpreted when enforcing contracts?
- Electronic signatures
    - UNCITRAL Model Law on Electronic Commerce
    - U.S. Code defines an electronic signature for the purpose of US law as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." 15 U.S.C. § 7006(5)
    - In the United States, the definition of what qualifies as electronic signature is wide and is set out in the Uniform Electronic Transactions Act (UETA)
    - Under UETA, the term means "an electronic sound, symbol, or process, attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record”