ISR Mites Concerns

Concerned ISR Citizens

7/5/2021

Context. We are writing to express our concerns about the Mites deployment in TCS Hall, as well as the way the deployment and concerns about it were handled. The Mites platform (https://mites.io/) is a small device that is installed on the inner walls of a building and measures temperature, humidity, pressure, light levels, color, and vibrations. It also has a low-resolution thermal camera and a microphone for sound. The purpose of the research is to help manage and optimize buildings for resident comfort, cost, etc.

The Mites sensors have been installed throughout the new TCS Hall, including in public spaces, meeting rooms, and private offices. Residents of private offices will have the opportunity to control the software on the Mite in their office in order to disable or enable different sensors, and perhaps eventually to enable smart building applications. By default, all the sensors of a Mite will be on and collect data except the microphone. If the microphone is turned on, the data is processed to make it difficult to extract data such as voices, but still allow detecting things like doors opening. Additional information is available at the Mites website above and in the Mites FAQ.

A group of 9 concerned faculty, staff, and students in ISR met last week. This document was written by a subset of that group in order to communicate the concerns brought up at that meeting to the larger community. Members of this group do not all feel exactly the same way about the Mites project. In the paragraphs below that start with “some of us,” subsequent occurrences of “we” mean the subgroup that is concerned about that issue. But we each share one or more of the concerns expressed in this document and we all believe that these concerns are reasonable and need to be heard and taken seriously by the community and departmental leadership.

We would like to say up front that we believe our colleagues doing the research are acting in good faith, and we want to support them in doing good science. Nevertheless, even someone with the best of intentions may take imperfect actions, and we do have real concerns about what is going on, as detailed below. We divide those into concerns about individual impact, about societal impact, about impact on CMU and ISR, about process, and about human subjects and consent.

Concerns about Individual Impact

Privacy and security. The sensors are designed with attention to privacy. However, some of us believe that significant risks remain. The devices are installed in every office, and they have microphones, which have the ability to gather sensitive data--even if the current firmware immediately scrambles it. There is no hardware off switch, the devices are network-connected, and they can be upgraded over the air. We understand that security best practices are being followed, but as any computer security expert knows, that is not a guarantee: you have to consider the worst case that is enabled by the hardware in the hands of a bad actor, not just the best case of what the software is meant to do when crafted by a good actor. So there is a security risk, even if low, that someone could hack into the system and reprogram a device to extract actual audio. This could be done even if the user “opts out” of having the microphone or other sensors on, because if there is an outside hacker (or an insider threat from the Mites development team) they can bypass the opt-out.

Some might assess the likelihood of this threat to be relatively low--probably similar to the threat of compromise of other electronic devices, such as a cell phone or laptop, that most of us routinely use. However, the consequences are high, because of the private space these sensors are in, and note that compromising a laptop affects only that user’s laptop, whereas compromising the Mites system could lead to compromising every sensor in the building. Also note that it is not only the PI’s assessment of risk that matters; according to the principle of Respect for Persons as autonomous agents (see the Belmont report), the subject’s assessment of risk also ought to be considered, and some subjects will assess this risk as being higher than what a given expert might say. We think this is a very reasonable “ask” in a setting with consent. But these devices have been put in offices without consent, and this is not a risk TCS residents should be required to take if they do not consent to it.

Moral injury. Moral injury can occur as a result of being asked to participate in activities, observe activities, or consider ideas or situations that the participant would find morally problematic or deeply against their values. As described below, some of us do see the deployment of devices such as these to be deeply against our values. We are nevertheless forced into a situation where such a device is in our office--even if the device is programmed not to take measurements. Even if the Mites in our offices are powered off, the sensors in public spaces or other offices will still collect data on us. Although this data is unlikely to be personally identifiable, we still feel that we are being forced to participate in a research program that we view as immoral.

Psychological harms. People who are concerned about surveillance are likely to feel significant stress and anxiety about having a mite in their office or in public spaces. Researchers have shown, for example, that people who believe they are being monitored in the workplace fear to express emotion [Pou09]. This anxiety can be real even for mites that are off, or mites that are on but not actively taking measurements. Some of us believe this might lead to some people being less likely to come to their offices, creating isolation from the collegial atmosphere we hope to create and affecting productivity. We believe forcing these people to accept a mite in their office or workplace will cause them psychological harm.

Ability to track individuals. The FAQ maintains that it would be prohibitively difficult to associate sensor data with individuals or locations due to the featurization and security protocols used. However, during times of low occupancy, for example, in the middle of the night when the only person in the building is a custodian, some of us are concerned that a bad actor could track that individual's movements through the building. The Mites FAQ #U5 states that mites data are tagged with locations, meaning it is possible to identify individuals with high likelihood, based on the office where they spend most of their time.

Major inconvenience to others' research subjects. Some members of our department conduct privacy research, including interviews with people who are very privacy-sensitive. They are concerned that those people will not be comfortable in a room that has a sensor in it, but all rooms in TCS (including private meeting rooms) will have such sensors. These members of the department will therefore have to conduct interviews outside TCS Hall, which is a major inconvenience. This is not speculation--PI Agarwal explicitly suggested this solution to the problem in a town hall meeting for graduate students. The concern also applies in an instructional setting, both for the classrooms in TCS and for instructors holding office hours or confidential meetings with students who may not be comfortable with the Mites.

Concerns about Societal Impact

Ethical concerns about the technology. Some of us feel that a network-connected software controllable microphone or a low-resolution thermal camera is an intrinsic violation of privacy, regardless of whether it is off or not. We do not want to live in a world where microphones and cameras (of any form and resolution) are present in offices.

This deep ethical concern means that some of us would simply like the Mites project to end, with all Mites removed from the building. At the same time, recognizing that this would mean the end of a major investment, research project, and dissertation project for the researchers, some of us do not want to push for this as an outcome, even as we recognize that it is a real and valid viewpoint.

Effect of CMU and ISR endorsing this research on wider societal and research norms. Related to the above, there are some who feel that a department at CMU installing microphones and low-resolution infrared cameras in private offices without consent may expand the kind of sensors which are normal in society or similar research, making it more likely that they are non-consensually installed in other spaces. CMU's brand is strong, and the argument “CMU did it, so we can too” carries weight.

Concerns about Impact on CMU and ISR

Effect on CMU/ISR's relationship to others. Multiple concerns have been brought up around how having the Mites sensors may impact the relationship of ISR with the world at large.

Some of us are concerned with the effect this may have on recruiting a strong and intellectually diverse community. After a group of REU students read the Mites FAQ using the link posted on public signage, at least two REU students have expressed concerns directly (six more through those two) about the Mites sensors. Will the presence of the Mites shape the people who choose to join our community as students or as employees? Can we welcome all different kinds of views? This is related to the sensors themselves, but also the way these issues have been handled (see "Concerns about Process" section).

Some of us feel that TCS is an outlier, as the only building on campus where you might imagine wanting to sign a consent form to walk in the door. Right now, we have a building that will feel hostile to some potential students and visiting scholars and we stick out substantially from the rest of the campus culture in this way. We do cutting edge Privacy research in ISR, and we are concerned that the quality of this research will suffer with a lower diversity of views as people silently choose a department without mandatory microphones or low-resolution infrared cameras in their office.

Finally, CMU is one of the top universities in computer science around the world, and ISR has the best privacy research. Some of us feel that it is ironic that ISR is hosting a project that some of its members feel does not respect their privacy. In the sense of research and social impact, researchers should not only investigate how powerful IoT devices could be, since industrial companies have already shown the power of big data without respecting privacy. As ISR researchers, we should demonstrate to the world that, to achieve the same goal of an IoT device, privacy should be and can be respected. And hopefully, we can lead the community to move forward towards a better direction.

Reputational Risk To ISR and CMU. Some of us see these sensors and practices as so far outside norms of acceptability so as to constitute a reputational risk to ISR or CMU if written about in national publications.

Concerns about Process

Involvement of stakeholders and process failure. Very little information was provided about the sensors before and during the move to TCS, and some of us believe this led to confusion and distrust. It gave us the sense that the project was following a regulatory framework instead of trying to understand and accommodate the concerns of the community.

There were missed opportunities to do this outreach. The researchers could have held a town hall on the research project for the entire ISR community before the decision was made to deploy Mites in TCS Hall. Such a town hall could have been very useful to the researchers--for example, it might have indicated the need for a physical on-off switch on the sensors, and they could have been manufactured with that in place. After informing the community, a vote could have been taken, with all faculty, staff, and students, as a way of gathering consent for the public data gathering in the project (we recognize this is not “normal procedure” for research projects, but Mites is far more intrusive than any other human subjects research project we are aware of at CMU). As it was, the first notification of the Mites sensors to the entire community was in August 2020, at which point the sensors were already installed and it was too late to ask for consent, except after the fact. Even after that message, when some of us expressed concerns, we were told to wait until more information was provided, months later.

Although work is being done now to address concerns raised across the ISR community, it is harder to address numerous issues because the deployment has already taken place. We believe that the right solution would have been to have these conversations much earlier, but that was impossible because of how and when the community was informed and consulted. We should continue to work towards greater transparency and community collaboration on a project that elicits strong ideological reactions from some individuals. The department should recognize and apologize for this lapse.

Use of data. For what purpose the data are collected and how the data will be processed are not clear to some of us. From different sources, people have talked about different research goals. However, this is concerning because the data may include PII (see below) which means the researchers should request consent from the participants and be clear about the purpose of use. Also, when the research goal changes, the changes should be made public and new consent should be requested. Moreover, when one decides to drop out from the experiment or leave the department, they should have the right to delete all the data related to them (e.g. all data collected in the Mite in their office).

Lifecycle and maintainability. Some of us are concerned about what happens to the Mites if the PIs of the Mites project chooses to leave CMU, or when the graduate students involved graduate. What happens to the data that was collected, which as described below, we believe constitutes identifiable private information? Who is going to monitor the sensors to make sure no bad actors have access to them? Will they be removed from the building?

Departmental response to concerns. Some of us feel that much of the response from departmental leadership, particularly when concerns were first being raised, has revolved around insinuating that concerns were unreasonable or misinformation, rather than engaging with the ideas underlying the concerns and coming to shared agreements. We recognize that bringing concerns to social media was escalatory (though not necessarily improper). However, given the little transparency and information about these sensors up to that point as well as the critical attitude many in the department hold towards IOT, privacy, and surveillance, there was a disappointing lack of engagement with concerns and criticisms.

The poor response was deeply exacerbated by the power imbalances here in ISR. Some students who had concerns about the sensors felt intimidated into silence after seeing the disciplinary action (including a highly inappropriate Doctoral Student Review letter) served to one of the most outspoken students. This intimidation impinges on the academic freedom of those who have concerns about this research project. In addition, staff members and others who may not feel they have the same academic freedoms have to make a far riskier decision to speak up.

Concerns about Human Subjects Research and Consent

Human subjects research not labeled as such. Some of us are concerned that the devices in default mode constitute human subjects research, even though they are not being labeled that way by the researchers and by the IRB. Federal regulations say that human subjects research takes place if an investigator conducts research that “Obtains information or biospecimens through intervention or interaction with [a living] individual, and uses, studies, or analyzes the information or biospecimens; or Obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens." We are concerned that both conditions hold about the Mites: they are an intervention, and they collect identifiable private information. We have talked with a researcher whose specialty is studying the ethics of human subjects research, and that researcher agrees with our concern.

The presence of sensors in offices--where these particular sensors, or any sensor with a microphone, would not ordinarily be present--is an intervention, and the purpose of the intervention is to gather data, including data that is impacted by and provides insight into human behavior. When one of us talked with the head of CMU’s IRB, it appeared that they have chosen to define “intervention” narrowly, to include only interventions where the researcher is comparing two conditions, but it is our understanding that there is no definition of the term in the law or regulations that would preclude “intervention” from covering significant changes to the environment of a subject. Likewise, the Mites FAQ#1 assumes that “intervention” means “an attempt to modify behavior or outcomes,” but we do not see any rationale in applicable law or regulations to limit the word intervention to so narrow a meaning (and neither does the expert ethicist we talked with). We did find a definition of “intervention” in the Common Rule: “Intervention includes both physical procedures by which information or biospecimens are gathered (e.g., venipuncture) and manipulations of the subject or the subject’s environment that are performed for research purposes” In the case of mites, the subject’s environment has been manipulated, for research purposes, by adding a Mite to their office.

Regarding the second definition of human subjects research, private information is defined to include “information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place.” The Mites can tell whether someone is occupying their office and where they are in it; an office is an environment with an expectation for privacy, so this is clearly private information. Identifiable private information is defined as “private information for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information." We understand from Mites FAQ #U5 that data from Mites devices is tagged with the location of the sensor. For private offices, this means the data is associated with an identifiable person: the occupant of the office. For shared offices, the data is associated with one of a small number of occupants. The Mites are thus collecting identifiable private information.

Thus, in contrast to Mites FAQ#1, we believe there is a clear case that the default Mites deployment is human subjects research by both federal definitions of the term. We are of course concerned that CMU's IRB determined that it is not. But IRBs are imperfect, and sometimes approve research that is in fact unethical, or judge research to be not human subjects research when it actually is (the recent University of Minnesota Linux security research debacle is an example). And even when IRBs interpret federal regulations correctly, those regulations only address a subset of ethical concerns. The burden of scrutiny for ethical concerns falling outside of the scope of IRB review falls to researcher's colleagues, peer reviewers, and wider research community.

More broadly, TCS is acting in a more informal sense as a "living laboratory" for the Mites. This is exciting! But also, many of us believe that we are the subjects of this experiment. We believe that a reasonable person who learns that a sensor has been installed in their office (or perhaps even in public spaces) for research purposes, and that the sensor can detect things like when they enter or leave the office, or their location within it, would consider themselves to be the subject of a research experiment. As James Davis wrote about the University of Minnesota case, `If humans feel they have been experimented on, we should call this "human-subjects research" — despite what the authors, UMN's IRB, and the research community say.' Following the Belmont Report's principle of Respect for Persons as autonomous individuals, the PI should respect this and should treat the research as if it were a human subjects study, even if his personal belief is that it is not.

The need for consent. Because some of us believe the deployment of Mites is human subjects research, we believe it requires consent of the subjects. The Common Rule states that a waiver of informed consent may be granted only if all of the following are true:

1. the research involves no more than minimal risk to the subjects;
2. the waiver or alteration will not adversely affect the rights and welfare of the subjects;
3. the research could not practicably be carried out without the waiver or alteration; and
4. whenever appropriate, the subjects will be provided with additional pertinent information after participation

Regarding the first point, while experts may disagree on the level of risk, it is indisputably true that some of us believe the research poses more than a minimal risk to us. So out of the Respect for Persons principle from the Belmont report, the first point should be taken to be false. Regarding the second point, a waiver of informed consent does adversely affect our rights and welfare, because it forces subjects to live with a sensor in their office even if that causes psychological harm, moral injury, and/or perceived risks to privacy. So the second point is also false. The third point is clearly false as well: the researchers could remove sensors from offices where a subject objects to their presence. We do not agree that this is impractical: removing or installing a sensor can safely be done in minutes with the kind of expertise that many department members possess. If the department wants to shield the PI from responsibility to do this, department staff could take care of this. So on all three counts--any one of which individually is sufficient--this research requires informed consent.

We are not the first to make this observation. When considering the use of nanosensors for health monitoring in the workplace, for example, Marchart proposes “Voluntary, not mandatory, participation” as a best practice for legal and ethical use [Mar19].

Obtaining informed consent from new community members. The ISR community changes over time as students apply and graduate, and faculty and staff are hired and leave. It is critical that someone who is considering joining our community fully understand the nature of the space they will be expected to work in. Some of us are concerned that the exact nature, and even existence of, of the Mites.io program is opaque to prospective new community members, some of whom may well disagree with it strongly enough to choose to not join ISR. Choosing to join ISR is not in and of itself a form of consent, especially when the details of the program are not made known.

Any job posting--staff, faculty, or otherwise--that will entail working in TCS spaces should inform someone applying for that job about the data that Mites will gather about them so that they can make an informed decision about if they want to join our community. Likewise, graduate programs with students in TCS need to make the conditions of the space clear to applying students.

Once a particular person is hired or accepted to a program, detailed information about the Mites.io project should be part of their onboarding and orientation. If they have any concerns, those need to be addressed, and if consent is needed from them it can be requested at that time.

Visitors outside the ISR community. Many people who are not affiliated with ISR frequent TCS, including custodial staff, collaborators, undergraduate and masters students, and family members (some of whom are minors and can’t consent). Some of us are concerned that these people are not consulted as stakeholders and will not be able to control the data collected from them. Many of them may not even be aware that data collection is happening, let alone make a decision of whether this is something they are comfortable with (though the signs that were put up are a start).

Actionable Next Steps Suggested

Members of the group collectively have a number of suggestions and requests to make of the PI and departmental leadership. One or more of us ask each of the following:

- That the Mites meeting on Tuesday, July 6, be an open conversation composed of two-way dialog with community members, rather than being dominated by a presentation on the research (as some of us feel was the case with past town halls). That more meetings be held if this discussion is cut short, to allow remaining dialog to occur.

- That the ISR department leadership acknowledge that the concerns outlined above are reasonable and real, even if they disagree with them. That departmental leadership make a public apology for prior communications that were dismissive of these concerns and had an intimidating effect on members of the department.

- That the faculty remove the problematic text from the inappropriate Doctoral Student Review letter from the student's permanent record.

- That the PI acknowledge that some members of the department see the Mites deployment as human subjects research, and that he agree to treat it as human subjects research that requires consent--even if the IRB does not require him to do so.

- That members of the department who want sensors physically removed from their office have the ability to do so. That opt-out requests (software or physical) be routed through an ombudsperson, not through the PI or his team, in order to maintain confidentiality about who made the request. That opt-out requests be handled in a timely manner (e.g. 1-2 business days) and that there is a way to verify they have been carried out. That a physical off switch be added to sensors in meeting rooms so that members and visitors to the department can opt out. That completed opt-out requests include a possibly optional marking on the space subsequent to the opt-out, indicating that the mites in that space are not active.

- That the PI consider mechanisms to allow subjects to consent to and/or opt out of data collection in public spaces. That the PI consider the feasibility of an off-switch in offices, as some of us are willing to consent to the Mite in our office but don't want to force our visitors to do so. Some of us believe it is essential for off switches to be part of all future deployments of Mites-like technologies, whether research or commercial.

- That further measures be taken to increase the transparency and openness of this project. These measures could include (and certainly would not be limited to) open sourcing the code for inspection, having an independent security audit on the code, or providing dashboards showing what kinds of data are being collected or stored and the granularity/format of the data (for example, storing the number of bluetooth devices is very different than storing the specific MAC addresses for bluetooth devices). Further, that the PI consider explaining in more detail what is actually being done with the data, and announce to the community when use of the data changes.

- That job postings and academic program descriptions where a successful application would result in being in any space with Mites sensors be amended to include a description of the program, the sort of data being collected, and a request for consent so that applicants can make an informed decision about joining the ISR community.

- That a lifecycle plan for both the sensors and data collected from them be developed, with community involvement, and made public so that it is clear what happens when the project ends or the goals of the project change.
- That durable signage be designed with community involvement and deployed throughout TCS and at all entrances, clearly and concisely stating what data is being collected about anyone who enters the space, how to opt out, and what rights people have over the data gathered about them.

References

[Mar19] Gary E. Marchart. What Are Best Practices for Ethical Use of Nanosensors for Worker Surveillance? AMA J Ethics. 2019;21(4):E356-362. doi: 10.1001/amajethics.2019.356.

[Pou09] Poullet Y. Data protection legislation: What is at stake for our society and democracy? Comput Law Secur Rev 2009; 25:211–226.