From: Leslie Peterson <leslieapeterson1@gmail.com>
Sent: Tuesday, December 01, 2020 5:09 PM
To: All Alders
Subject: Vote YES on Agenda item #76

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders and Mayor,

I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments-Agenda item #76. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance. If the amendments come into play, I would ask that you vote NO on the alternate proposed ordinance (submitted by Alder Henak) and vote YES on the 2nd substitute ordinance (submitted by the authors of the original proposal - Alders Kemble, Prestigiacomo, Evers, Verveer, Foster and Heck). I won't add anything else here, as I would like to keep this communication brief. Facial recognition technology can be used to destroy civil rights and increase police power at a time when we should be exploring alternatives designed to positively impact all members of society.
Thank you for your public service.

Leslie Peterson
District 12

Veldran, Lisa

From: JACK K PHILLIPS <jack.phillips@wisc.edu>
Sent: Wednesday, November 18, 2020 4:01 PM
To: PD PSRC; Evers, Tag; Mayor; All Alders
Subject: Facial Recognition

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Hello,

I'd just like to say that I fully support banning use of facial recognition surveillance by the city, and especially by MPD. This surveillance technology, pushed by large out-of-state corporations like Amazon, removes any ability for citizens to opt out of invasive data collection. It acts as a black box, a Robocop, which removes accountability for police when the technology makes mistakes, as it so often does, especially when attempting to distinguish people of color. The legal and regulatory framework for facial recognition surveillance is sparse at best, allowing for unnecessary and disproportionate surveillance of law-abiding citizens, and creating tenuous justifications for the incarceration of activists, which deters citizens from exercising their right to free speech. As mentioned, this method of surveillance frequently cannot distinguish people of color, leading to illegitimate arrests of innocent people from marginalized groups already facing undue repression from police, and sentenced based on automation bias, the belief that technology is infallible, if they are lucky enough to survive their arrest. How long until another Tony Robinson, until a young man is gunned down by police led to the incorrect address by inaccurate surveillance technology? Please vote to ban this dangerous surveillance technology from our city, and continue the great work of the Public Safety Review Committee under the leadership of Brenda Konkel.

-Jack

Mx. Jack K. Phillips
They/Them
Graduate Student, Biomedical Engineering
University of Wisconsin-Madison

From: CALM@iavwav.com
Sent: Monday, November 23, 2020 3:03 PM
To: All Alders
Subject: [All Alders] Facial Recognition Ban

Recipient: All Alders

Name: Cal Mazzara
Address: 3001 PERRY ST, MADISON, WI 53713
Phone: 605-509-2605
Email: CALM@IAVWAV.COM

Would you like us to contact you? Yes, by email

Message:

Good Day,
My name is Cal Mazzara from Wisconsin Audio Video in Madison. I saw on the news the other night about the concerns about facial recognition and that there is a proposed ban.
I share the same concerns you do over this technology, however, I happen to be a designer of systems that use facial recognition in a way that dispels all the concerns people have with this technology. My partners at Verkada have created a system that started out with the facial recognition concerns people have. In short, you CAN have a facial recognition system that does not impede on people's rights. And as far as racial bias goes...it wont and can't really be biased based on the technology.
I would like to talk to you more about this. There are several stories I wish to share where this technology saved lives, saved items from theft, and has done so much good in the communities they serve. All without impeding people's privacy rights.
Please call me at 608-509-2605. I would love to show you how it CAN be done the right way.
Thank you for your time. I look forward to hearing from you.

Veldran, Lisa

From: Amelia Royko Maurer <roykomaurer@mac.com>
Sent: Wednesday, November 18, 2020 1:28 PM
To: All Alders
Subject: Facial Recognition Software

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders,

Please vote against city-use of facial recognition software. The harm caused by this technology far outweighs any benefits. If MPD didn't engage so heavily in confirmation bias, this matter wouldn't even be on the table.

This technology is especially harmful to BIPOC communities. It's not a matter of opinion, it's a fact.

Every vote against White Supremacy Racism matters. Every. Single. One. This one too. No excuses!

I've copied an exerpt from Dr Greg Gelembiuk's letter. As per usual, he's done his homework.

"**1.** Here is a column by Anna Lauren Hoffmann, an assistant professor in the University of Washington Information School.

https://static1.squarespace.com/.../HoffmannSeattleTimesF...

Excerpt:

The dangers of facial recognition technology cannot be overstated. Prominent critics point to pernicious biases — especially against dark skin or young faces — that haven't been adequately addressed. When tested, Amazon's own "Rekognition" system falsely matched more than two dozen members of the United States Congress with criminal mug shots, including a disproportionate number of members of the Congressional Black Congress. Further work has shown how such systems confuse cultural markers of gender or sexuality (like makeup and hairstyles) with physiological ones, effectively "baking in" harmful stereotypes that limit their effectiveness across populations.

More importantly, facial recognition is not happening in a vacuum. It is plugging into existing surveillance structures that threaten millions of Americans daily, enabling the real-time monitoring of individuals by instantly linking faces up to the many information systems already available. One glance, and your face can be tied quickly to local law enforcement records, FBI files, DMV data, financial information, social media profiles, and more.

None of this is hypothetical. Many state and local police departments already have much of this access — they just need your face to supercharge it.

Worse, these structures are already marked by deep inequality. Surveilling Americans has always been a skewed affair, with certain groups bearing more of the burden than others — from persistent monitoring of religious minorities and communities of color to the invasive questioning heaped upon the poor to the systematic tracking of protesters exercising their rights to speech and assembly. Such inequality cannot be addressed by mere "tweaks" to the system. In fact, if facial recognition worked flawlessly, it would only make matters worse. It would simply "perfect" unfair and stifling patterns of targeting and abuse aimed at historically vulnerable populations.

Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium. Passing watered-down and permissive versions of the bill now will only allow face recognition to penetrate deeper into our lives while unmaking any appetite we might have for regulation in the first place.

As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.

2. 40 groups have called for a US moratorium on facial recognition technology. The groups include the Electronic Freedom Foundation, the Consumer Federation of America, the Freedom of the Press Foundation, Media Alliance, the National LGBTQ Task Force and Patient Privacy Rights.

Article: https://www.technologyreview.com/.../facial-recognition.../

Letter from the 40 groups: https://epic.org/.../face.../PCLOB-Letter-FRT-Suspension.pdf

3. Here is an article by Malkia Devich-Cyril, entitled "Defund Facial Recognition. I'm a second-generation Black activist, and I'm tired of being spied on by the police."

https://www.theatlantic.com/.../defund-facial.../613771/...

4. Article by Birgit Schippers (in the U.K.) "Facial recognition: ten reasons you should be worried about the technology"

https://theconversation.com/facial-recognition-ten...

Excerpt:

The right to privacy matters, even in public spaces. It protects the expression of our identity without uncalled-for intrusion from the state or from private companies. Facial recognition technology's indiscriminate and large-scale recording, storing and analysing of our images undermines this right because it means we can no longer do anything in public without the state knowing about it."

Sincerely,

Amelia Royko Maurer

Veldran, Lisa

From:	Alisha Steele <steele1of12@yahoo.com>
Sent:	Wednesday, November 18, 2020 7:27 PM
To:	All Alders
Subject:	against funding facial recognition

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Alders,

I am writing to register my opposition to the funding and use of facial recognition technology in the city. There are better investments for our city to make.

Alisha Steele
1421 Pleasure Drive
Madison WI 53704

From:	T Clemente <tclemente@rocketmail.com>
Sent:	Wednesday, November 18, 2020 7:43 PM
To:	All Alders
Subject:	Fw: Support Agenda Item 4 - banning facial recognition

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Good evening, I am forwarding my email to the PDPSRC as this will be coming before you soon.

----- Forwarded Message -----
From: T Clemente <tclemente@rocketmail.com>
To: "pdpsrc@cityofmadison.com" <pdpsrc@cityofmadison.com>
Sent: Wednesday, November 18, 2020, 4:57:26 PM CST
Subject: Support Agenda Item 4 - banning facial recognition

Good afternoon,

I am writing to you to ask that you SUPPORT Agenda Item #4 at tonight's meeting, as written, a full ban. Facial recognition technology is riddled with serious problems and should not be implemented. As stated by Anna Lauren Hoffmann, an assistant professor at the University of Washington Information School puts it, "The dangers of facial recognition technology cannot be overstated." She points to the fact that when Amazon's "Rekognition" system was tested it "falsely matched more than two dozen members of the United States Congress with criminal mug shots, including a disproportionate number of members of the Congressional Black Caucus."

While members of the United States Congress have ample ability to hire professional attorneys should they be falsely accused by this technology to clear their names, the VAST majority of members of our community do not. Please support Agenda Item 4. Thank you for your time.

Trina Clemente
2601 Myrtle St
Madison, WI 53704

Veldran, Lisa

From: Bonnie Roe <bonnie.roe@gmail.com>
Sent: Wednesday, November 25, 2020 10:42 AM
To: Mayor; Bottari, Mary; All Alders
Subject: Please table proposed ban on Facial Recognition Technology

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Mayor Satya Rhodes-Conway, Ms. Bottari, and Alders,

I am a Madison resident of 21 years, writing with grave concerns about the proposed overreaching, city-wide ban on Facial Recognition Technology. Like other technologies, facial recognition can be misused, but I believe those risks can be minimized while still giving Law Enforcement the ability to use cutting-edge technology to fight our most serious crimes.

The suggested language in the new substitute seems far too limited:"

(4) Exemptions. This Section does not apply to the following:
(a) Using information evidence relating to the investigation of a specific crime that
may have been generated from a face surveillance system, so long as
such information evidence was not generated by or at the request of any
Department and is used only to identify individuals who are victims of
human trafficking or missing children."

It would tie the hands of MPD at tracking down our most vulnerable victims and lose the ability to generate tips on confirmed suspects. One concern is it could limit the police department from initiating a third-party FRT involvement if that request does not come from someone outside of the police department. If the police department has a strong lead, it would be a shame to pass up that technology simply because an outside request doesn't make initiation, or to even be able to mention it to, say, parents of child victims. Why? Who does it help? Who does it hurt?

Another concern I have is the way this limits the use of FRT in violent crimes or other serious (felony) cases. For example, the case of Althea Bernstein, who had reported 4 white frat boys yelled a racial slur at her, poured lighter fluid on her and lit her face on fire. What if something had been captured on surveillance cameras at that intersection? It would be a hate crime. Would we not want to be able to add a FRT search to potentially help identify those suspects? I like how Chief Wahl referred to it as just one piece of evidence. It's not like DNA which can seal the deal, it is merely an investigative lead to be added to the mix of potential evidence/further research. If every other agency is banned, that is fine by me, but MPD alone is tasked with public safety and enforcing the law.

In the case of an active shooter, imminent threat, mass casualty event or other serious felonies, this technology could be vital. I imagine there could even be liability issues to an outright ban on its use.

I understand the civil rights concerns and agree we must not be scanning groups of protesters or random residents through this software, etc. It should not be used for racial profiling, for people exercising their First Amendment rights, for petty crimes, or used in a random nature to build a database of faces. It should be evaluated case-by-case, as it pertains to a specified suspect or victim, so that it does not become commonplace. I like that MPD policy is that the Chief of Police needs to be consulted before the technology is requested for use by an external software company. I think having an agreement, with oversight, between MPD and the City is a vital safeguard so that it is not misused. Facial recognition tools and policies could be made open to independent review by the Oversight Committee. This new and evolving technology is not going away. In a free-market society, strong governance is the way to benefit from the positive aspects of FRT while providing a robust defense against its improper use.

I hope this Ordinance can be tabled for more time for discussion, public input, and most importantly, collaboration with MPD on how this will affect their fight against violent crime. Of course they will continue to do what they can even without this ever-improving technology, but it will be a needless drain on time and resources when an image could turn up a potential match in minutes. Sometimes in this fight, time is of the essence. If it does come down to a vote on Tuesday night, I urge you to vote no. This ban is too limiting and a real threat to public safety.

In case it helps, I am including the link of the most recent Public Safety Review Committee below. The presentation by Chief Victor Wahl and Sergeant Detective Julie Johnson was very informative and well done. It starts at 2:39:47 in the linked video.

https://media.cityofmadison.com/Mediasite/Showcase/madison-city-channel/Presentation/53936094156545ca8b9ede98d5a75e731d

Thank you for your consideration,
Bonnie Roe
608-239-1748

From:	LN Alliet <lnalliet@gmail.com>
Sent:	Thursday, November 26, 2020 8:28 AM
To:	All Alders; Bottari, Mary; Rhodes-Conway, Satya V.
Subject:	Support the ban of facial recognition technology by the City of Madison

Caution: This email was sent from an external source. Avoid unknown links and attachments.

I am writing to register my strong support for the ban of the use of facial recognition technology by the City of Madison. This item should be adopted as written without modifications or changes.

I am deeply disappointed with the Mayor's Office's proposed alternative language which gravely endangers our friends, neighbors, and residents, especially those of color. I am upset by MPD's assertion about the use of the technology in child sex trafficking cases, without any data or examples - and in direct contradiction to the research on facial recognition technology.

Please support the ban of the use of facial recognition technology by the City of Madison (currently listed as item #76 of the agenda).

Thank you,
Lee Alliet

4737 Sherwood Road, Madison

Veldran, Lisa

From:	Amber Dwyer <amber.shane@gmail.com>
Sent:	Thursday, November 26, 2020 8:36 AM
To:	All Alders; Bottari, Mary; Rhodes-Conway, Satya V.
Subject:	Support the ban of facial recognition technology by the City of Madison

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Hello,

I am writing to register my strong support for the ban of the use of facial recognition technology by the City of Madison. This item should be adopted as written without modifications or changes.

I am deeply disappointed with the Mayor's Office's proposed alternative language which gravely endangers our friends, neighbors, and residents, especially those of color. I am upset by MPD's assertion about the use of the technology in child sex trafficking cases, without any data or examples, and in direct contradiction to the research on facial recognition technology.

Please support the ban of the use of facial recognition technology by the City of Madison (currently listed as item #76 of the agenda).

Thank you,
Amber Dwyer

1446 Bellflower Ln., Madison

From:	Jen Gaber <jlgaber@gmail.com>
Sent:	Thursday, November 26, 2020 11:52 AM
To:	All Alders; Rhodes-Conway, Satya V.; Bottari, Mary

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders and Mayor,

I am writing to ask that you support the proposed ordinance to prohibit the use of artificial intelligence facial recognition technology by city departments. Use of facial recognition software would be several steps backward for Madison. If you have read up on the subject before your meeting; you already know that facial recognition software makes a lot of mistakes. False identification of a victim or a perpetrator will be very traumatic for Madison and the individuals involved, and will have serious consequences.

An examination of facial identification software at MIT found an error rate of 0.8% for light skinned men and 34.7% for dark skinned women. Use of such technology goes against any Madison effort to bridge racial gaps in equity and justice. We already have social instability in Madison. We already have tremendous work to do on racial inequity. We cannot accept such flawed, untested, and unregulated technology companies taking a support role in our law enforcement agencies. At the **very least** we must wait a good long time to observe and study its use and where this goes.

This tool is inaccurate and the way these companies handle data is very questionable.

We would be better off to adopt a Biometric Information Privacy Act like Illinois has or banning local government agencies' use of facial recognition technology as San Francisco has. The exchange of freedom and privacy for this anecdotal evidence of usefulness is unacceptable. You will see, across the nation, cities and states fighting against its use. Please join them, and support prohibiting use of AI facial recognition technology in our community.

We can do better than this. Please, do better.

--
Jennifer Gaber
608.622.4138
3210 Quincy Ave.
Madison, WI 53704

From:	Ryan Hartkopf <ryanhartkopf@gmail.com>
Sent:	Thursday, November 26, 2020 5:05 PM
To:	All Alders
Subject:	Support for facial recognition ban

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Hello Alders,

I am writing in support for the ban on facial recognition software. We are already struggling with disproportionate outcomes along racial lines in the state of Wisconsin, Dane county, and the city of Madison. Why would we then implement technologies that have massive error rates for people who are not white?

Please review this story of mistaken identity that resulted from use of faulty facial recognition technology. We don't need more innocent people being arrested.

https://web.archive.org/web/20201027065132if_/https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/

Thank you,

Ryan Hartkopf
6633 Raymond Rd
Madison, WI

Veldran, Lisa

From:	Jake Winkler <trappedinink@gmail.com>
Sent:	Thursday, November 26, 2020 6:12 PM
To:	All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject:	Face Surveillance Ban

Caution: This email was sent from an external source. Avoid unknown links and attachments.

In considering the ordinance, the first question ought to be if the tool can make things better or worse. When this came up in committee, the industry representative said the top algorithms have no bias. He cited NIST reporting, represented here, which tested nearly 200 algorithms. You'll note that any time the article says bias is small or negligible, that's true for ~5-7 (<5%) of the algorithms. This "small bias" claim is also qualified every time: at a specific error threshold, or only true for *most* demographics. Even when they do, the error rate was often 3x higher for non-white male groups (eg the sentences preceding footnoes 11 and 13) So even the best don't work well in all scenarios, and how do we know we'll get one of the best algorithms?

This NIST article (Dec 2019) talks about accuracy being determined by 3 factors: the algorithm itself, the application that uses it, and the data it's fed. Assuming Madison in the future allows an algorithm that shows negligible bias and high accuracy, what guarantees do citizens have that the other two factors will also be high quality? The "data it's fed" is especially concerning because we'll have a low quality source image from a security camera or cell phone video that we're trying to match against some database of images. What is that database? Whatever MPD has available, which is likely a population biased towards people that already have encounters with these systems, eg mugshots. If you had a database of the entire population of Dane County, that would be a far more reasonable pool to go fishing in. The book Automating Inequality points out that when your search database is skewed to people with contact with criminal justice or social services, you're going to compound their hardships when a robot says there's a chance they are the person in the video, then they can be detained and questioned and have their life interrupted and miss work.

The ordinance amendments address some of the "it's too broad" charges brought up, namely that authenticating users is allowed, as is current MPD's use of a third party that uses the tech.

This tool seems like a waste of money and will create more problems than it solves in its current accuracy levels.

From: Ken Swift <kswift@uwalumni.com>
Sent: Friday, November 27, 2020 12:29 AM
To: All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject: Facial Recognition

Dear Alders and Mayor Satya,

Please support the ordinance to ban facial recognition tools as there are too many reasons for even considering okaying it. In the majority of cases IT DOESN'T WORK! Studies have definitively shown that it fails most of the time. Read the letter from Greg Gelembiuk for better details. It can't be stated any better than that. The technology is flawed and even if made better it smacks of dictatorial rule. Not okay, good Alders and Mayor Satya.

Thank you for supporting and protecting your/our citizens of Madison.

Ken Swift
Rutledge St. 03

Veldran, Lisa

From:	Trisha Patterson <mywavetp@gmail.com>
Sent:	Friday, November 27, 2020 9:26 AM
To:	All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject:	Facial recognition- NO

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders and Mayor,

I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

As Robert Williams, a Black Detroit resident, writes in a Washington Post article:

I was wrongfully arrested because of facial recognition. Why are police allowed to use it?... Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed. What's worse is that, before this happened to me, I actually believed them. I thought, what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?

Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.

The ACLU states:

We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.

Institutions such as the Georgetown Law Center on Privacy and Technology are also calling for a ban, noting that "a dramatic range of abuse and bias has surfaced". As Lindsey Barret of Georgetown Law Center writes in the publication "Ban Facial Recognition Technologies for Children – and Everyone Else":

Clearview AI, which has been heavily criticized for its privacy violative services, has been quick to tout the use of its product in cases involving children, including investigations into child sexual exploitation. The horrendous nature of those crimes may seem to reduce the need for scruples when it comes to the harms of these technologies, when in fact the sensitivity of the circumstances makes their problems even more concerning. The false identification of a victim could be deeply traumatic, and the false identification of an ostensible perpetrator could lead to tremendously damaging consequences for the wrongly identified.

Anna Lauren Hoffmann, a professor at University of Washington Information School, writes:

Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium…. As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.

Facial recognition software produces inaccurate and biased results.

Some people have a mistaken belief that facial recognition technology works as it's portrayed in TV shows like NCIS. Such shows are science fiction – reality is totally different.

Inaccuracy is particularly high with children and the elderly. The 2019 NIST (National Institute of Standards and Technology) report shows that if you use ideal photos (i.e., the best possible conditions) for both a test photo of a child and a database of photos of different children, the typical vendor algorithm will incorrectly call 1% of all photos in the database a match (making this technology close to useless for children). There's also racial bias - existing facial recognition software exhibit greatly elevated error rates with faces of Black folks, and especially Black women.

Moreover, as one article notes of the NIST findings...

accuracy is only possible in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the subjects are clear and unobscured. In real world deployments, accuracy rates tend to be far lower. For example, the FRVT [2019 NIST Facial Recognition Vendor Test] found that the error rate for one leading algorithm climbed from 0.1% [for middle-aged adults] when matching against high-quality mugshots to 9.3% when matching instead to pictures of individuals captured 'in the wild,' where the subject may not be looking directly at the camera or may be obscured by objects or shadows.

Thus, a 2018 study by a British nonprofit found:

The overwhelming majority of the police's "matches" using automated facial recognition to date have been inaccurate. On average, a staggering 95% of "matches" wrongly identified innocent people… Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people.

Police face recognition will disproportionately harm Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals.

Facial recognition technology constitutes a grave danger to civil liberties

Facial recognition technology infringes on a vital constitutional principle, the right to privacy, raising serious 4th amendment issues. It can permit cataloging of sensitive information and unchecked location tracking. And it can profoundly impact 1st amendment rights - endangering and chilling 1st amendment activities and press freedoms.

In their article "Facial Recognition Is the Perfect Tool for Oppression", Woodrow Hartzog (Professor of Law and Computer Science at Northeastern University School of Law) and Evan Selinger (Professor of Philosophy at Rochester Institute of Technology) note:

facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented. It's the missing piece in an already dangerous surveillance infrastructure, built because that infrastructure benefits both the government and private sectors. And when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering….

It's easy to think people don't have a strong privacy interest in faces because many of us routinely show them in public…. The thing is we actually do have a privacy interest in our faces, and this is because humans have historically developed the values and institutions associated with privacy protections during periods where it's been difficult to identify most people we don't know. Thanks to biological constraints, the human memory is limited; without technological augmentation, we can remember only so many faces. And thanks to population size and distribution, we'll encounter only so many people over the course of our lifetimes. These limitations create obscurity zones.

The Project On Government Oversight (POGO), a nonpartisan watchdog, has issued a report entitled "Facing the Future of Surveillance". It starkly outlines several of the severe dangers to liberty posed by facial recognition technology. Here's an excerpt:

In last year's landmark Supreme Court decision Carpenter v. United States, the Supreme Court took on the novel risks surveillance in the digital age pose, fully embracing the right to privacy. In an opinion focused on cellphone tracking, the Court declared that "the [Fourth] Amendment seeks to secure the privacies of life against arbitrary power" (emphasis added), a framing that notably focuses not on certain places or types of conversation, but rather on protecting details of each person's life against an ever-watching government. Perhaps even more explicitly, the opinion of the Court in Carpenter stated that "a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance.",,,,

When the Court in Carpenter highlighted that location records "hold for many Americans the privacies of life" (emphasis added), it was emphasizing that Fourth Amendment privacy protections do not focus narrowly on privately owned places, but rather on people themselves, wherever they may be.... In Carpenter, the Court highlighted that "a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner," and therefore presents heightened risks to privacy. While cell phones may have become an extension of our bodies, our faces require no such metaphor; unlike cellphones, our faces are never able to be turned off, left behind, or cast aside. If our faces can be subjected to the same type of continuous surveillance as cellphones, strong limits on surveillance technology will be necessary to properly rebalance power between the government and the people....

Facial recognition amplifies the concerns of upending privacy and unbalancing power between the government and its citizens in a unique and especially troubling way. The Supreme Court's key fear in both Jones and Carpenter was that in the course of tracking location, the government would unearth individuals' most sensitive activities. As Justice Sotomayor highlighted, this form of surveillance could catalog "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."... Such data could be used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to applications for background checks, to evaluations for civil service employment opportunities. Equally important is the potentially chilling effect on political and other types of participation, such as religious and community activities....

Facial recognition surveillance threatens to become as powerful a method of finding and tracking individuals as are cellphone and GPS tracking. While the Supreme Court has imposed a warrant requirement for these other forms of electronic location tracking, no such limit exists for facial recognition. In time, facial recognition could become a uniquely powerful location-tracking tool because there is no "middle man" for government-managed cameras that controls access to the data; the entire surveillance system is managed and all relevant information is obtained directly by law enforcement...

A necessary aspect of freedom of expression and association is group anonymity. Over six decades ago, the Supreme Court held that "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." In that case, NAACP v. Alabama, the key action at issue was the government demanding NAACP's Alabama membership list. In the digital age, no such direct action is necessary to remove the anonymity of an organization's members. A single camera outside the entrance or exit to a group's events combined with facial recognition could produce a membership list without consent or even notification. And because such identification can be done with practically no expenditure of human resources, it can be conducted on a mass scale....

Facial recognition could be a tool to disrupt First Amendment-protected activities. Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and then arrest any individual with an active bench warrant. Ability to effortlessly identify any bench warrant for any petty offense could enable arbitrary action and abusive targeting, such as against selectively targeted individuals attending "events of interest," such as protests, political events, and religious ceremonies. This was already observed on a small scale with Geofeedia—a social media-monitoring company—which admitted that Baltimore police used the service during protests to "run social media photos through facial recognition technology" to find individuals with "outstanding warrants and arrest them directly from the crowd," with the goal of targeting individuals who were protesting. Given the number of bench warrants for petty offenses that some municipalities maintain, it is entirely possible that facial recognition could become an "arrest-at-will" authority used to disrupt such activities on a broad basis....

Modern surveillance powers force journalists to take extra precautions, such as leaving cell phones and other electronic devices with built in GPS at home. But facial recognition can be used not just to catalog activities, but also interactions. If it becomes a tool to pinpoint how individuals interact and meet with journalists, it could present significant roadblocks for journalists seeking to speak to sources and whistleblowers while preserving anonymity.

Face surveillance is a menace disguised as a gift. Its implementation threatens to leave us all less free. Please support a strict ban on the use of this violative technology.

Sincerely,

— with Jesse Pycha-Holst and 57 others.

From: KRISTIN MATHEWS <imkrzy4mm@att.net>
Sent: Sunday, November 29, 2020 9:00 AM
To: All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject: Face surveillance technology

Dear Alders and Mayor,

I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

I personally have a friend who was wrongfully arrested based on inaccurate facial recognition technology. I would never wish the trauma that he endured on anyone.

Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.

Inaccuracy is particularly high with children and the elderly. The 2019 NIST (National Institute of Standards and Technology) report shows that if you use ideal photos (i.e., the best possible conditions) for both a test photo of a child and a database of photos of different children, the typical vendor algorithm will incorrectly call 1% of all photos in the database a match (making this technology close to useless for children). There's also racial bias - existing facial recognition software exhibit greatly elevated error rates with faces of Black folks, and especially Black women.

Face surveillance is a menace disguised as a gift. Its implementation threatens to leave us all less free. Please support a strict ban on the use of this violative technology.

Sincerely,

Kristin Mathews, 1133 Northland Dr, Madison 53704

MEDIUM.COM

Facial Recognition Is the Perfect Tool for Oppression

With such a grave threat to privacy and civil liberties, measured regulation should be abandoned in favor of an outright ban

22Amelia Royko Maurer, Leslie Amsterdam and 20 others
7 Comments
15 Shares

Like

Comment

Share

Comments

View 3 more comments

[Ken Swift]

Done and done. Wow, Greg, that was a dozen grand slams you provided up there. As ever we thank you for teaching us.

3

○ **Like**

○ ·

Reply

○ ·

Share

○ · 2d

[Leslie Amsterdam]

[Greg]

,thanks for doing the heavy lifting so that we participate more fully!

○ **Like**

○ ·

Reply

○ ·

Share

○ · 9m

Write a comment...

-
-
-
-

Unread Announcements ·54

See All

Log in to Facebook

New Activity

About

All posts to this page must be relevant to the work and mission of the Madison Community Response Team

Community Response Team Mission Stateme…
See More

Public

Anyone can see who's in the group and what

Veldran, Lisa

From: Erin Lemley <afuzzybird@gmail.com>
Sent: Sunday, November 29, 2020 9:49 AM
To: All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject: I Support the Full Ban on Facial Recognition

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Madison Alders and Mayor Rhodes-Conway,

I am writing in support of a complete ban of the use of facial recognition software by city departments, including the police department. This technology is fraught with problems and biases, and is likely to cause serious problems for our Black neighbors. Facial recognition technology has high racially-based error rates, and we have a disproportionate number of Black faces already in our mug shot databases. In addition, constant surveillance is against our constitutional right to "be secure in their persons...against unreasonable searches and seizures" (Amendment IV). No citizen, Black, white, young or old should be subjected to the use of facial recognition software. We have a right to privacy in our lives.

Although the police department would have you believe that they need this technology to track down child sex offenders, the reality is that facial recognition works particularly poorly for children. This appeal is made to tug at our heartstrings and have us ignore our logical minds.The horrific nature of child sex crimes means that incorrectly identifying a victim or falsely accusing someone based on facial recognition software can lead to lifelong trauma. We should not be supporting this.

In addition, I do not support any alternative language for this bill. Giving the police department the ability to use this software for "large scale events" means that our citizens who are peacefully protesting are at risk for retaliation. This is not acceptable.

Please vote for a full, strict ban on facial recognition technology without any exceptions for the Madison Police Department. Support the freedom of your citizens--the risks and harms of facial recognition greatly outweigh any perceived benefits.

Sincerely,
Erin M Lemley
1703 Rowland Ave #1
Madison, WI 53704
District 15

Veldran, Lisa

From:	DJH Photo <djhphoto@hotmail.com>
Sent:	Sunday, November 29, 2020 11:47 AM
To:	All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject:	I Support #76 to ban use of facial recognition technology by the City of Madison
Importance:	High

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear City Aders and Mayor Rhodes-Conway,

I am writing you all today to express my support for item #76 on this coming Tuesday's Agenda.

SUBSTITUTE - Creating Section 23.63 of the Madison General Ordinances establishing a Ban on the Use of Face Surveillance Technology.

Please support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

As Robert Williams, a Black Detroit resident, writes in a Washington Post article:

I was wrongfully arrested because of facial recognition. Why are police allowed to use it?... Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed. What's worse is that, before this happened to me, I actually believed them. I thought, what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?

Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.

The ACLU states:

We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.

Institutions such as the Georgetown Law Center on Privacy and Technology are also calling for a ban, noting that "a dramatic range of abuse and bias has surfaced". As Lindsey Barret of Georgetown Law Center writes in the publication "Ban Facial Recognition Technologies for Children – and Everyone Else": Clearview AI, which has been heavily criticized for its privacy violative services, has been quick to tout the use of its product in cases involving children, including investigations into child sexual exploitation. The horrendous nature of those crimes may seem to reduce the need for scruples when it comes to the harms of these technologies, when in fact the sensitivity of the circumstances makes their problems even more concerning. The false identification of a victim could be deeply traumatic, and the false identification of an ostensible perpetrator could lead to tremendously damaging consequences for the wrongly identified.

Anna Lauren Hoffmann, a professor at University of Washington Information School, writes:

Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium.... As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.

Facial recognition software produces inaccurate and biased results.

Some people have a mistaken belief that facial recognition technology works as it's portrayed in TV shows like NCIS. Such shows are science fiction – reality is totally different.

Inaccuracy is particularly high with children and the elderly. The 2019 NIST (National Institute of Standards and Technology) report shows that if you use ideal photos (i.e., the best possible conditions) for both a test photo of a child and a database of photos of different children, the typical vendor algorithm will incorrectly call 1% of all photos in the database a match (making this technology close to useless for children). There's also racial bias - existing facial recognition software exhibit greatly elevated error rates with faces of Black folks, and especially Black women.

Moreover, as one article notes of the NIST findings...

accuracy is only possible in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the subjects are clear and unobscured. In real world deployments, accuracy rates tend to be far lower. For example, the FRVT [2019 NIST Facial Recognition Vendor Test] found that the error rate for one leading algorithm climbed from 0.1% [for middle-aged adults] when matching against high-quality mugshots to 9.3% when matching instead to pictures of individuals captured 'in the wild,' where the subject may not be looking directly at the camera or may be obscured by objects or shadows.

Thus, a 2018 study by a British nonprofit found:

The overwhelming majority of the police's "matches" using automated facial recognition to date have been inaccurate. On average, a staggering 95% of "matches" wrongly identified innocent people... Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people. Police face recognition will disproportionately harm Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals. Facial recognition technology constitutes a grave danger to civil liberties Facial recognition technology infringes on a vital constitutional principle, the right to privacy, raising serious 4th amendment issues. It can permit cataloging of sensitive information and unchecked location tracking. And it can profoundly impact 1st amendment rights - endangering and chilling 1st amendment activities and press freedoms.

In their article "Facial Recognition Is the Perfect Tool for Oppression", Woodrow Hartzog (Professor of Law and Computer Science at Northeastern University School of Law) and Evan Selinger (Professor of Philosophy at Rochester Institute of Technology) note: facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented. It's the missing piece in an already dangerous surveillance infrastructure, built because that infrastructure benefits both the government and private sectors. And when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering....

It's easy to think people don't have a strong privacy interest in faces because many of us routinely show them in public.... The thing is we actually do have a privacy interest in our faces, and this is because humans have historically developed the values and institutions associated with privacy protections during periods where it's been difficult to identify most people we don't know. Thanks to biological constraints, the human memory is limited; without technological augmentation, we can remember only so many faces. And thanks to population size and distribution, we'll encounter only so many people over the course of our lifetimes. These limitations create obscurity zones.

The Project On Government Oversight (POGO), a nonpartisan watchdog, has issued a report entitled "Facing the Future of Surveillance". It starkly outlines several of the severe dangers to liberty posed by facial recognition technology.

Here's an excerpt:

In last year's landmark Supreme Court decision Carpenter v. United States, the Supreme Court took on the novel risks surveillance in the digital age pose, fully embracing the right to privacy. In an opinion focused on cellphone tracking, the Court declared that "the [Fourth] Amendment seeks to secure the privacies of life against arbitrary power" (emphasis added), a framing that notably focuses not on certain places or types of conversation, but rather on protecting details of each person's life against an ever-watching government. Perhaps even more explicitly, the opinion of the Court in Carpenter stated that "a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance."....

When the Court in Carpenter highlighted that location records "hold for many Americans the privacies of life" (emphasis added), it was emphasizing that Fourth Amendment privacy protections do not focus narrowly on privately owned places, but rather on people themselves, wherever they may be.... In Carpenter, the Court highlighted that "a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner," and therefore presents heightened risks to privacy. While cell phones may have become an extension of our bodies, our faces require no such metaphor; unlike cellphones, our faces are never able to be turned off, left behind, or cast aside. If our faces can be subjected to the same type of continuous surveillance as cellphones, strong limits on surveillance technology will be necessary to properly rebalance power between the government and the people....

Facial recognition amplifies the concerns of upending privacy and unbalancing power between the government and its citizens in a unique and especially troubling way. The Supreme Court's key fear in both Jones and Carpenter was that in the course of tracking location, the government would unearth individuals' most sensitive activities. As Justice Sotomayor highlighted, this form of surveillance could catalog "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."... Such data could be used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to applications for background checks, to evaluations for civil service employment opportunities. Equally important is the potentially chilling effect on political and other types of participation, such as religious and community activities....

Facial recognition surveillance threatens to become as powerful a method of finding and tracking individuals as are cellphone and GPS tracking. While the Supreme Court has imposed a warrant requirement for these other forms of electronic location tracking, no such limit exists for facial recognition. In time, facial recognition could become a uniquely powerful location-tracking tool because there is no "middle man" for government-managed cameras that controls access to the data; the entire surveillance system is managed and all relevant information is obtained directly by law enforcement...

A necessary aspect of freedom of expression and association is group anonymity. Over six decades ago, the Supreme Court held that "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." In that case, NAACP v. Alabama, the key action at issue was the government demanding NAACP's Alabama membership list. In the digital age, no such direct action is necessary to remove the anonymity of an organization's members. A single camera outside the entrance or exit to a group's events combined with facial recognition could produce a membership list without consent or even notification. And because such identification can be done with practically no expenditure of human resources, it can be conducted on a mass scale....

Facial recognition could be a tool to disrupt First Amendment-protected activities. Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and then arrest any individual with an active bench warrant. Ability to effortlessly identify any bench warrant for any petty offense could enable arbitrary action and abusive targeting, such as against selectively targeted individuals attending "events of interest," such as protests, political events, and religious ceremonies. This was already observed on a small scale with Geofeedia—a social media-monitoring company—which admitted that Baltimore police used the service during protests to "run social media photos through facial recognition technology" to find individuals with "outstanding warrants and arrest them directly from the crowd," with the goal of targeting individuals who were protesting. Given the number of bench warrants for petty offenses that some municipalities maintain, it is entirely possible that facial recognition could become an "arrest-at-will" authority used to disrupt such activities on a broad basis....

Modern surveillance powers force journalists to take extra precautions, such as leaving cell phones and other electronic devices with built in GPS at home. But facial recognition can be used not just to catalog activities, but also interactions. If it becomes a tool to pinpoint how individuals interact and meet with journalists, it could present significant roadblocks for journalists seeking to speak to sources and whistleblowers while preserving anonymity.

Face surveillance is a menace disguised as a gift. Its implementation threatens to leave us all less free. Please support a strict ban on the use of this violative technology.

Respectfully,

DJ Haugen
111 W Wilson Street #204
Madison, WI 53703
djhphoto@hotmail.com

Veldran, Lisa

From:	P Wehrle <pcwehrle@gmail.com>
Sent:	Sunday, November 29, 2020 12:50 PM
To:	All Alders; Mayor; Bottari, Mary
Subject:	Vote to Prohibit Facial Surveillance Technology

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders and Madam Mayor,

I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

As Robert Williams, a Black Detroit resident, writes in a Washington Post article:
I was wrongfully arrested because of facial recognition. Why are police allowed to use it?... Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed. What's worse is that, before this happened to me, I actually believed them. I thought, what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?
Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.

The police have many other tools at their disposal.This is an unnecessary incursion into the privacy of citizens. We do not need to become a surveillance state to be safe.

Thank You,

Peter Lawrence-Wehrle
3310 Cross Street
Madison, WI 53711

Veldran, Lisa

From:	Angela Witt <angelakwitt@gmail.com>
Sent:	Sunday, November 29, 2020 3:21 PM
To:	All Alders; Rhodes-Conway, Satya V.
Subject:	Facial recognition ban

Dear Alders and Mayor,

I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. The ordinance has been written to allow MPD to use face surveillance evidence provided by other organizations, so long as MPD hasn't requested it, and the authors are amending the ordinance to allow MPD to specifically request face surveillance searches to identify individuals who are victims of human trafficking or child sexual exploitation, or missing children. Please do not weaken this ordinance.

Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.

The ACLU states:
We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.

Inaccuracy is particularly high with children and the elderly. The 2019 NIST (National Institute of Standards and Technology) report shows that if you use ideal photos (i.e., the best possible conditions) for both a test photo of a child and a database of photos of different children, the typical vendor algorithm will incorrectly call 1% of all photos in the database a match (making this technology close to useless for children). There's also racial bias - existing facial recognition software exhibit greatly elevated error rates with faces of Black folks, and especially Black women.

Moreover, as one article notes of the NIST findings...
accuracy is only possible in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the subjects are clear and unobscured. In real world deployments, accuracy rates tend to be far lower. For example, the FRVT [2019 NIST Facial Recognition Vendor Test] found that the error rate for one leading algorithm climbed from 0.1% [for middle-aged adults] when matching against high-quality mugshots to 9.3% when matching instead to pictures of individuals captured 'in the wild,' where the subject may not be looking directly at the camera or may be obscured by objects or shadows.

Police face recognition will disproportionately harm Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals.

Facial recognition technology constitutes a grave danger to civil liberties. Facial recognition technology infringes on a vital constitutional principle, the right to privacy, raising serious 4th amendment issues. It can permit cataloging of sensitive information and unchecked location tracking. And it can profoundly impact 1st amendment rights - endangering and chilling 1st amendment activities and press freedoms.

The Project On Government Oversight (POGO), a nonpartisan watchdog, has issued a report entitled “Facing the Future of Surveillance”. It starkly outlines several of the severe dangers to liberty posed by facial recognition technology, including the potential for privacy violations and a chilling effect on political, religious, and community activities potentially subject to surveillance.

Face surveillance threatens everyone's freedom, and is likely to disproportionately harm those already suffering disproportionate harm from policing. Please support a strict ban on its use.

Sincerely,
Angela Witt
Madison, WI

Veldran, Lisa

From:	Daniel Bock <danielbockwi@gmail.com>
Sent:	Sunday, November 29, 2020 4:14 PM
To:	All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject:	Item 76 on Tuesday

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders and Mayor,

I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

As Robert Williams, a Black Detroit resident, writes in a Washington Post article:
I was wrongfully arrested because of facial recognition. Why are police allowed to use it?... Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed. What's worse is that, before this happened to me, I actually believed them. I thought, what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?
Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.
The ACLU states:
We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.
Institutions such as the Georgetown Law Center on Privacy and Technology are also calling for a ban, noting that "a dramatic range of abuse and bias has surfaced". As Lindsey Barret of Georgetown Law Center writes in the publication "Ban Facial Recognition Technologies for Children – and Everyone Else":
Clearview AI, which has been heavily criticized for its privacy violative services, has been quick to tout the use of its product in cases involving children, including investigations into child sexual exploitation. The horrendous nature of those crimes may seem to reduce the need for scruples when it comes to the harms of these technologies, when in fact the sensitivity of the circumstances makes their problems even more concerning. The false identification of a victim could be deeply traumatic, and the false identification of an ostensible perpetrator could lead to tremendously damaging consequences for the wrongly identified.
Anna Lauren Hoffmann, a professor at University of Washington Information School, writes:
Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium…. As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.
Facial recognition software produces inaccurate and biased results.
Some people have a mistaken belief that facial recognition technology works as it's portrayed in TV shows like NCIS. Such shows are science fiction – reality is totally different.
Inaccuracy is particularly high with children and the elderly. The 2019 NIST (National Institute of Standards and Technology) report shows that if you use ideal photos (i.e., the best possible conditions) for both a test photo of a child and a database of photos of different children, the typical vendor algorithm will incorrectly call 1% of all photos in the database a match (making this technology close to useless for children). There's also racial bias - existing facial recognition software exhibit greatly elevated error rates with faces of Black folks, and especially Black women.

Moreover, as one article notes of the NIST findings...

accuracy is only possible in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the subjects are clear and unobscured. In real world deployments, accuracy rates tend to be far lower. For example, the FRVT [2019 NIST Facial Recognition Vendor Test] found that the error rate for one leading algorithm climbed from 0.1% [for middle-aged adults] when matching against high-quality mugshots to 9.3% when matching instead to pictures of individuals captured 'in the wild,' where the subject may not be looking directly at the camera or may be obscured by objects or shadows.

Thus, a 2018 study by a British nonprofit found:

The overwhelming majority of the police's "matches" using automated facial recognition to date have been inaccurate. On average, a staggering 95% of "matches" wrongly identified innocent people... Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people.

Police face recognition will disproportionately harm Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals.

Facial recognition technology constitutes a grave danger to civil liberties

Facial recognition technology infringes on a vital constitutional principle, the right to privacy, raising serious 4th amendment issues. It can permit cataloging of sensitive information and unchecked location tracking. And it can profoundly impact 1st amendment rights - endangering and chilling 1st amendment activities and press freedoms.

In their article "Facial Recognition Is the Perfect Tool for Oppression", Woodrow Hartzog (Professor of Law and Computer Science at Northeastern University School of Law) and Evan Selinger (Professor of Philosophy at Rochester Institute of Technology) note:

facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented. It's the missing piece in an already dangerous surveillance infrastructure, built because that infrastructure benefits both the government and private sectors. And when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering....

It's easy to think people don't have a strong privacy interest in faces because many of us routinely show them in public.... The thing is we actually do have a privacy interest in our faces, and this is because humans have historically developed the values and institutions associated with privacy protections during periods where it's been difficult to identify most people we don't know. Thanks to biological constraints, the human memory is limited; without technological augmentation, we can remember only so many faces. And thanks to population size and distribution, we'll encounter only so many people over the course of our lifetimes. These limitations create obscurity zones.

The Project On Government Oversight (POGO), a nonpartisan watchdog, has issued a report entitled "Facing the Future of Surveillance". It starkly outlines several of the severe dangers to liberty posed by facial recognition technology. Here's an excerpt:

In last year's landmark Supreme Court decision Carpenter v. United States, the Supreme Court took on the novel risks surveillance in the digital age pose, fully embracing the right to privacy. In an opinion focused on cellphone tracking, the Court declared that "the [Fourth] Amendment seeks to secure the privacies of life against arbitrary power" (emphasis added), a framing that notably focuses not on certain places or types of conversation, but rather on protecting details of each person's life against an ever-watching government. Perhaps even more explicitly, the opinion of the Court in Carpenter stated that "a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance.",,,,

When the Court in Carpenter highlighted that location records "hold for many Americans the privacies of life" (emphasis added), it was emphasizing that Fourth Amendment privacy protections do not focus narrowly on privately owned places, but rather on people themselves, wherever they may be.... In Carpenter, the Court highlighted that "a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner," and therefore presents heightened risks to privacy. While cell phones may have become an extension of our bodies, our faces require no such metaphor; unlike cellphones, our faces are never able to be turned off, left behind, or cast aside. If our faces can be subjected to the same type of continuous surveillance as cellphones, strong limits on surveillance technology will be necessary to properly rebalance power between the government and the people....

Facial recognition amplifies the concerns of upending privacy and unbalancing power between the government and its citizens in a unique and especially troubling way. The Supreme Court's key fear in both Jones and Carpenter was that in the course of tracking location, the government would unearth individuals' most sensitive activities. As Justice Sotomayor highlighted, this form of surveillance could catalog "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."... Such data could be used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to applications for background checks, to evaluations for civil service employment opportunities. Equally important is the potentially chilling effect on political and other types of participation, such as religious and community activities....

Facial recognition surveillance threatens to become as powerful a method of finding and tracking individuals as are cellphone and GPS tracking. While the Supreme Court has imposed a warrant requirement for these other forms of electronic location tracking, no such limit exists for facial recognition. In time, facial recognition could become a uniquely powerful location-tracking tool because there is no "middle man" for government-managed cameras that controls access to the data; the entire surveillance system is managed and all relevant information is obtained directly by law enforcement...

A necessary aspect of freedom of expression and association is group anonymity. Over six decades ago, the Supreme Court held that "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." In that case, NAACP v. Alabama, the key action at issue was the government demanding NAACP's Alabama membership list. In the digital age, no such direct action is necessary to remove the anonymity of an organization's members. A single camera outside the entrance or exit to a group's events combined with facial recognition could produce a membership list without consent or even notification. And because such identification can be done with practically no expenditure of human resources, it can be conducted on a mass scale....

Facial recognition could be a tool to disrupt First Amendment-protected activities. Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and then arrest any individual with an active bench warrant. Ability to effortlessly identify any bench warrant for any petty offense could enable arbitrary action and abusive targeting, such as against selectively targeted individuals attending "events of interest," such as protests, political events, and religious ceremonies. This was already observed on a small scale with Geofeedia—a social media-monitoring company—which admitted that Baltimore police used the service during protests to "run social media photos through facial recognition technology" to find individuals with "outstanding warrants and arrest them directly from the crowd," with the goal of targeting individuals who were protesting. Given the number of bench warrants for petty offenses that some municipalities maintain, it is entirely possible that facial recognition could become an "arrest-at-will" authority used to disrupt such activities on a broad basis....

Modern surveillance powers force journalists to take extra precautions, such as leaving cell phones and other electronic devices with built in GPS at home. But facial recognition can be used not just to catalog activities, but also interactions. If it becomes a tool to pinpoint how individuals interact and meet with journalists, it could present significant roadblocks for journalists seeking to speak to sources and whistleblowers while preserving anonymity.

Face surveillance is a menace disguised as a gift. Its implementation threatens to leave us all less free. Please support a strict ban on the use of this violative technology.

Sincerely,

Daniel Bock - Madison, WI resident

Veldran, Lisa

From:	Esty Dinur <eedinur99@gmail.com>
Sent:	Sunday, November 29, 2020 10:40 PM
To:	All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject:	Ordinance to ban use of facial recognition technology by the City of Madison

Dear Alders and Mayor,

I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

As Robert Williams, a Black Detroit resident, writes in a Washington Post article:

I was wrongfully arrested because of facial recognition. Why are police allowed to use it?... Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed. What's worse is that, before this happened to me, I actually believed them. I thought, what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?

Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.

The ACLU states:

We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.

Institutions such as the Georgetown Law Center on Privacy and Technology are also calling for a ban, noting that "a dramatic range of abuse and bias has surfaced". As Lindsey Barret of Georgetown Law Center writes in the publication "Ban Facial Recognition Technologies for Children – and Everyone Else":

Clearview AI, which has been heavily criticized for its privacy violative services, has been quick to tout the use of its product in cases involving children, including investigations into child sexual exploitation. The horrendous nature of those crimes may seem to reduce the need for scruples when it comes to the harms of these technologies, when in fact the sensitivity of the circumstances makes their problems even more concerning. The false identification of a victim could be deeply traumatic, and the false identification of an ostensible perpetrator could lead to tremendously damaging consequences for the wrongly identified.

Anna Lauren Hoffmann, a professor at University of Washington Information School, writes:

Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium.... As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.

Facial recognition software produces inaccurate and biased results.

Some people have a mistaken belief that facial recognition technology works as it's portrayed in TV shows like NCIS. Such shows are science fiction – reality is totally different.

Inaccuracy is particularly high with children and the elderly. The 2019 NIST (National Institute of Standards and Technology) report shows that if you use ideal photos (i.e., the best possible conditions) for both a test photo of a child and a database of photos of different children, the typical vendor algorithm will incorrectly call 1% of all photos in the database a match (making this technology close to useless for children). There's also racial bias - existing facial recognition software exhibit greatly elevated error rates with faces of Black folks, and especially Black women.

Moreover, as one article notes of the NIST findings...

accuracy is only possible in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the subjects are clear and unobscured. In real world deployments, accuracy rates tend to be far lower. For example, the FRVT [2019 NIST Facial Recognition Vendor Test] found that the error rate for one leading algorithm climbed from 0.1% [for middle-aged adults] when matching against high-quality mugshots to 9.3% when matching instead to pictures of individuals captured 'in the wild,' where the subject may not be looking directly at the camera or may be obscured by objects or shadows.

Thus, a 2018 study by a British nonprofit found:

The overwhelming majority of the police's "matches" using automated facial recognition to date have been inaccurate. **On average, a staggering 95% of "matches" wrongly identified innocent people**... Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people.

Police face recognition will disproportionately harm Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals.

Facial recognition technology constitutes a grave danger to civil liberties

Facial recognition technology infringes on a vital constitutional principle, the right to privacy, raising serious 4th amendment issues. It can permit cataloging of sensitive information and unchecked location tracking. And it can profoundly impact 1st amendment rights - endangering and chilling 1st amendment activities and press freedoms.

In their article "Facial Recognition Is the Perfect Tool for Oppression", Woodrow Hartzog (Professor of Law and Computer Science at Northeastern University School of Law) and Evan Selinger (Professor of Philosophy at Rochester Institute of Technology) note:

facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented. It's the missing piece in an already dangerous surveillance infrastructure, built because that infrastructure benefits both the government and private sectors. And when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering....

It's easy to think people don't have a strong privacy interest in faces because many of us routinely show them in public.... The thing is we actually do have a privacy interest in our faces, and this is because humans have historically developed the values and institutions associated with privacy protections during periods where it's been difficult to identify most people we don't know. Thanks to biological constraints, the human memory is limited; without technological augmentation, we can remember only so many faces. And thanks to population size and distribution, we'll encounter only so many people over the course of our lifetimes. These limitations create obscurity zones.

The Project On Government Oversight (POGO), a nonpartisan watchdog, has issued a report entitled "Facing the Future of Surveillance". It starkly outlines several of the severe dangers to liberty posed by facial recognition technology. Here's an excerpt:

In last year's landmark Supreme Court decision Carpenter v. United States, the Supreme Court took on the novel risks surveillance in the digital age pose, fully embracing the right to privacy. In an opinion focused on cellphone tracking, the Court declared that "the [Fourth] Amendment seeks to secure **the *privacies of life*** against arbitrary power" (emphasis added), a framing that notably focuses not on certain places or types of conversation, but rather on protecting details of each person's life against an ever-watching government. Perhaps even more explicitly, the opinion of the Court in Carpenter stated that "a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance.",,,,

When the Court in Carpenter highlighted that location records "hold for many Americans **the privacies of life**" (emphasis added), it was emphasizing that Fourth Amendment privacy protections do not focus narrowly on privately owned places, but rather on people themselves, wherever they may be.....In Carpenter, the Court highlighted that "a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner," and therefore presents heightened risks to privacy. While cell phones may have become an extension of our bodies, our faces require no such metaphor; unlike cellphones, our faces are never able to be turned off, left behind, or cast aside. If our faces can be subjected to the same type of continuous surveillance as cellphones, strong limits on surveillance technology will be necessary to properly rebalance power between the government and the people....

Facial recognition amplifies the concerns of upending privacy and unbalancing power between the government and its citizens in a unique and especially troubling way. The Supreme Court's key fear in both Jones and Carpenter was that in the course of tracking location, the government would unearth individuals' most sensitive activities. As Justice Sotomayor highlighted, this form of surveillance could catalog "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."... Such data could be used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to applications for background checks, to evaluations for civil service employment opportunities. Equally important is the potentially chilling effect on political and other types of participation, such as religious and community activities....

Facial recognition surveillance threatens to become as powerful a method of finding and tracking individuals as are cellphone and GPS tracking. While the Supreme Court has imposed a warrant requirement for these other forms of electronic location tracking, no such limit exists for facial recognition. In time, facial recognition could become a uniquely powerful location-tracking tool because there is no "middle man" for government-managed cameras that controls access to the data; the entire surveillance system is managed and all relevant information is obtained directly by law enforcement...

A necessary aspect of freedom of expression and association is group anonymity. Over six decades ago, the Supreme Court held that "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." In that case, NAACP v. Alabama, the key action at issue was the government demanding NAACP's Alabama membership list. In the digital age, no such direct action is necessary to remove the anonymity of an organization's members. A single camera outside the entrance or exit to a group's events combined with facial recognition could produce a membership list without consent or even notification. And because such identification can be done with practically no expenditure of human resources, it can be conducted on a mass scale....

Facial recognition could be a tool to disrupt First Amendment-protected activities. Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and then arrest any individual with an active bench warrant. Ability to effortlessly identify any bench warrant for any petty offense could enable arbitrary action and abusive targeting, such as against selectively targeted individuals attending "events of interest," such as protests, political events, and religious ceremonies. This was already observed on a small scale with Geofeedia—a social media-monitoring company—which admitted that Baltimore police used the service during protests to "run social media photos through facial recognition technology" to find individuals with "outstanding warrants and arrest them directly from the crowd," with the goal of targeting individuals who were protesting. Given the number of bench warrants for petty offenses that some municipalities maintain, it is entirely possible that facial recognition could become an "arrest-at-will" authority used to disrupt such activities on a broad basis....

Modern surveillance powers force journalists to take extra precautions, such as leaving cell phones and other electronic devices with built in GPS at home. But facial recognition can be used not just to catalog activities, but also interactions. If it becomes a tool to pinpoint how individuals interact and meet with journalists, it could present significant roadblocks for journalists seeking to speak to sources and whistleblowers while preserving anonymity.

Face surveillance is a menace disguised as a gift. Its implementation threatens to leave us all less free. Please support a strict ban on the use of this violative technology.

Sincerely,

--
Esty Dinur
District 18

From:	Carol Hermann <hermann.carol.l@gmail.com>
Sent:	Monday, November 30, 2020 1:30 AM
To:	All Alders; Bottari, Mary; Rhodes-Conway, Satya V.
Subject:	Facial recognition technology

Dear Mayor Rhodes-Conway and Council Members,

I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments, in keeping with recommendations from numerous civil rights organizations including the ACLU, Consumer Federation of America, and the Electronic Privacy Information Center.
Facial recognition software produces inaccurate and biased results, especially when used to identify people of color, and poses a threat to our civil liberties, including our right to privacy. Multiple studies have shown that under the best of circumstances this technology often produces false positive identifications and the potential for misuse and abuse far outweighs the benefits. Please pass the ordinance as written without amendment.

Thank you for your consideration,

Carol Hermann
2636 Quartz Rd, 53711

From:	Katrina Gray <okcallmegoddess@gmail.com>
Sent:	Monday, November 30, 2020 7:31 AM
To:	All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject:	Facial Recognition Technology

Caution: This email was sent from an external source. Avoid unknown links and attachments.

I am writing to encourage you to please pass the facial recognition ban as written. Banning this technology is in the best interest of all residents. It's important that the ban be passed as is and not watered down.

Katrina Gilliam
2138 Oakridge Ave
Madison, WI
53705

From: jhirsch@chorus.net
Sent: Monday, November 30, 2020 9:49 AM
To: Mayor; All Alders; Bottari, Mary
Subject: Oppose Item #76-Ban on Facial Surveillance

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Mayor and Alders:

I ask you to **OPPOSE Item #76** Establishing a Ban on the Use of Face Surveillance Technology which is on your December 1, 2020 agenda.

Understandably, there is a concern about how to balance individual privacy with the advantages that facial surveillance can bring to public safety and security. Before enacting a ban, I suggest that you evaluate the pros and cons of the broader category of biometrics. As technology advances, the uses continue to increase in both the private and public sectors.

As with the internet, there will be federal and state legislation to address some of the concerns. The development of some common procedures and implementation guidelines for all City departments should be considered. This will go a long way to assure Madison residents that the technology is being used appropriately.

For additional background, you can view the document "Facial Recognition Technology: Balancing Safety and Privacy" from the Wisconsin Legislative Reference Bureau at:

https://docs.legis.wisconsin.gov/misc/lrb/wisconsin_policy_project/facial_recognition_privacy_3_4.pdf

Let's keep Madison at the forefront of evolving technology.

Thank you.

Janet Hirsch
7311 Cedar Creek Trail
Madison, WI 53717

Veldran, Lisa

From:	Lena Haasl <lenaahaasl@gmail.com>
Sent:	Monday, November 30, 2020 11:19 AM
To:	All Alders
Subject:	Support the Ban on Face Surveillance Technology

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders and Mayor,

I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

As Robert Williams, a Black Detroit resident, writes in a Washington Post article:

I was wrongfully arrested because of facial recognition. Why are police allowed to use it?... Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed. What's worse is that, before this happened to me, I actually believed them. I thought, what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?

Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.

The ACLU states:

We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.

Institutions such as the Georgetown Law Center on Privacy and Technology are also calling for a ban, noting that "a dramatic range of abuse and bias has surfaced". As Lindsey Barret of Georgetown Law Center writes in the publication "Ban Facial Recognition Technologies for Children – and Everyone Else":

Clearview AI, which has been heavily criticized for its privacy violative services, has been quick to tout the use of its product in cases involving children, including investigations into child sexual exploitation. The horrendous nature of those crimes may seem to reduce the need for scruples when it comes to the harms of these technologies, when in fact the sensitivity of the circumstances makes their problems even more concerning. The false identification of a victim could be deeply traumatic, and the false identification of an ostensible perpetrator could lead to tremendously damaging consequences for the wrongly identified.

Anna Lauren Hoffmann, a professor at University of Washington Information School, writes:

Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium.... As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.

Facial recognition software produces inaccurate and biased results.

Some people have a mistaken belief that facial recognition technology works as it's portrayed in TV shows like NCIS. Such shows are science fiction – reality is totally different.

Inaccuracy is particularly high with children and the elderly. The 2019 NIST (National Institute of Standards and Technology) report shows that if you use ideal photos (i.e., the best possible conditions) for both a test photo of a child and a database of photos of different children, the typical vendor algorithm will incorrectly call 1% of all photos in the database a match (making this technology close to useless for children). There's also racial bias -

existing facial recognition software exhibit greatly elevated error rates with faces of Black folks, and especially Black women.

Moreover, as one article notes of the NIST findings...

accuracy is only possible in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the subjects are clear and unobscured. In real world deployments, accuracy rates tend to be far lower. For example, the FRVT [2019 NIST Facial Recognition Vendor Test] found that the error rate for one leading algorithm climbed from 0.1% [for middle-aged adults] when matching against high-quality mugshots to 9.3% when matching instead to pictures of individuals captured 'in the wild,' where the subject may not be looking directly at the camera or may be obscured by objects or shadows.

Thus, a 2018 study by a British nonprofit found:

The overwhelming majority of the police's "matches" using automated facial recognition to date have been inaccurate. On average, a staggering 95% of "matches" wrongly identified innocent people... Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people.

Police face recognition will disproportionately harm Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals.

Facial recognition technology constitutes a grave danger to civil liberties

Facial recognition technology infringes on a vital constitutional principle, the right to privacy, raising serious 4th amendment issues. It can permit cataloging of sensitive information and unchecked location tracking. And it can profoundly impact 1st amendment rights - endangering and chilling 1st amendment activities and press freedoms.

In their article "Facial Recognition Is the Perfect Tool for Oppression", Woodrow Hartzog (Professor of Law and Computer Science at Northeastern University School of Law) and Evan Selinger (Professor of Philosophy at Rochester Institute of Technology) note:

facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented. It's the missing piece in an already dangerous surveillance infrastructure, built because that infrastructure benefits both the government and private sectors. And when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering....

It's easy to think people don't have a strong privacy interest in faces because many of us routinely show them in public.... The thing is we actually do have a privacy interest in our faces, and this is because humans have historically developed the values and institutions associated with privacy protections during periods where it's been difficult to identify most people we don't know. Thanks to biological constraints, the human memory is limited; without technological augmentation, we can remember only so many faces. And thanks to population size and distribution, we'll encounter only so many people over the course of our lifetimes. These limitations create obscurity zones.

The Project On Government Oversight (POGO), a nonpartisan watchdog, has issued a report entitled "Facing the Future of Surveillance". It starkly outlines several of the severe dangers to liberty posed by facial recognition technology. Here's an excerpt:

In last year's landmark Supreme Court decision Carpenter v. United States, the Supreme Court took on the novel risks surveillance in the digital age pose, fully embracing the right to privacy. In an opinion focused on cellphone tracking, the Court declared that "the [Fourth] Amendment seeks to secure the privacies of life against arbitrary power" (emphasis added), a framing that notably focuses not on certain places or types of conversation, but rather on protecting details of each person's life against an ever-watching government. Perhaps even more explicitly, the opinion of the Court in Carpenter stated that "a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance.",,,,

When the Court in Carpenter highlighted that location records "hold for many Americans the privacies of life" (emphasis added), it was emphasizing that Fourth Amendment privacy protections do not focus narrowly on privately owned places, but rather on people themselves, wherever they may be.... In Carpenter, the Court highlighted that "a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner," and therefore presents heightened risks to privacy. While cell phones may have become an extension of our bodies, our faces require no such metaphor; unlike cellphones, our faces are never able to be turned off, left behind, or cast aside. If our faces can be subjected to the same type of continuous surveillance as cellphones, strong limits on surveillance technology will be necessary to properly rebalance power between the government and the people....

Facial recognition amplifies the concerns of upending privacy and unbalancing power between the government and its citizens in a unique and especially troubling way. The Supreme Court's key fear in both Jones and Carpenter was that in the course of tracking location, the government would unearth individuals' most sensitive activities. As Justice Sotomayor highlighted, this form of surveillance could catalog "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."... Such data could be used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to applications for background checks, to evaluations for civil service employment opportunities. Equally important is the potentially chilling effect on political and other types of participation, such as religious and community activities....

Facial recognition surveillance threatens to become as powerful a method of finding and tracking individuals as are cellphone and GPS tracking. While the Supreme Court has imposed a warrant requirement for these other forms of electronic location tracking, no such limit exists for facial recognition. In time, facial recognition could become a uniquely powerful location-tracking tool because there is no "middle man" for government-managed cameras that controls access to the data; the entire surveillance system is managed and all relevant information is obtained directly by law enforcement...

A necessary aspect of freedom of expression and association is group anonymity. Over six decades ago, the Supreme Court held that "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." In that case, NAACP v. Alabama, the key action at issue was the government demanding NAACP's Alabama membership list. In the digital age, no such direct action is necessary to remove the anonymity of an organization's members. A single camera outside the entrance or exit to a group's events combined with facial recognition could produce a membership list without consent or even notification. And because such identification can be done with practically no expenditure of human resources, it can be conducted on a mass scale....

Facial recognition could be a tool to disrupt First Amendment-protected activities. Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and then arrest any individual with an active bench warrant. Ability to effortlessly identify any bench warrant for any petty offense could enable arbitrary action and abusive targeting, such as against selectively targeted individuals attending "events of interest," such as protests, political events, and religious ceremonies. This was already observed on a small scale with Geofeedia—a social media-monitoring company—which admitted that Baltimore police used the service during protests to "run social media photos through facial recognition technology" to find individuals with "outstanding warrants and arrest them directly from the crowd," with the goal of targeting individuals who were protesting. Given the number of bench warrants for petty offenses that some municipalities maintain, it is entirely possible that facial recognition could become an "arrest-at-will" authority used to disrupt such activities on a broad basis....

Modern surveillance powers force journalists to take extra precautions, such as leaving cell phones and other electronic devices with built in GPS at home. But facial recognition can be used not just to catalog activities, but also interactions. If it becomes a tool to pinpoint how individuals interact and meet with journalists, it could present significant roadblocks for journalists seeking to speak to sources and whistleblowers while preserving anonymity.

Face surveillance is a menace disguised as a gift. Its implementation threatens to leave us all less free. Please support a strict ban on the use of this violative technology.

Sincerely,

Elena Haasl

Veldran, Lisa

From: Norm Sannes <norman.sannes@gmail.com>
Sent: Monday, November 30, 2020 12:00 PM
To: All Alders
Subject: Agenda Item: 76 62413 banning facial surveillance

Caution: This email was sent from an external source. Avoid unknown links and attachments.

I am opposed to banning facial recognition technology. It has proven very helpful in solving crimes. It's a tool that our law enforcement needs. It's pathetic that this proposal is even being considered.

</ Norman Sannes> 5345 Queenbridge Rd.Madison, WI

Veldran, Lisa

From:	rongratz@gmail.com
Sent:	Monday, November 30, 2020 12:01 PM
To:	All Alders
Subject:	[All Alders] Facial Recognition Cameras

Recipient: All Alders

Name: Ron Gratz
Address: 706 S. High Point Road, #310, Madison, WI 53719
Phone: 608-770-1359
Email: rongratz@gmail.com

Would you like us to contact you? No, do not contact me

Message:

Hello:

I wish to express my opposition regarding the proposed facial recognition ordinance. While I appreciate the concerns that the cameras/photos supporters have to not allow law enforcement to use these cameras, I strongly feel that they should be allowed in high level felony cases such as 1st and 2nd degree sexual assault, homicides including attempted. If the only piece of information that can provide a lead for law enforcement, why would even consider this to be a violation of an ordinance? Every possible avenue should be explored to bring someone to justice. Once a persons have been identified, the information alone cannot be enough to convict but can be substantial in forming a case and evidence to identify the suspect. What if it was your loved one, or friend, or colleague that was murdered or assaulted and the police were left with very little evidence but the facial recognition could help lead the investigation? Tell that to a parent that they cannot use the facial recognition program to identify a possible suspect or to create a lead!

Of course there need to be checks and balances but let the judge decide that, not YOU, the council. Put limitations on the use of the camera. You should never flat-out eliminate any possible evidence that can be used to identify a criminal.

Thank you!

Ron Gratz

Veldran, Lisa

From:	Xerxes Minocher <xminocher@gmail.com>
Sent:	Monday, November 30, 2020 12:37 PM
To:	All Alders
Subject:	Support Agenda Item #76 - Facial recognition ban

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Members of the Common Council,

I am writing to ask that you fully support Item 76 on the agenda tomorrow as written, with no further amendments. The ban on facial surveillance technology by all city departments including the police takes into account growing issues with this kind of technology, while still being flexible enough to allow the Madison PD to function and operate with its partners as before.

Portions of my PhD research focus on the use of technologies such as these by police departments across the country. As the Madison Police Chief and proponents have argued that such software is an especially helpful tool in certain child-search cases, we should first note the proposed ordinance does not interfere with such a use case.

There are several concerns with facial surveillance, recognition, and other automated and predictive technologies used in law enforcement throughout the country however, and these justify a ban.

1) Racial bias – this is perhaps the most obvious and popular critique against such systems. As it stands now, facial surveillance and recognition technologies throughout the country continue to suffer from an inability to accurately identify non-white individuals as accurately as white individuals. This is a result of designer bias, incomplete and disparate data being used to 'train' these technologies, and has already had negative, tangible effects on people of color. This alone should be enough reason to adopt the proposed ordinance banning facial surveillance in the city as proposed, with no further amendments.

2) Undue influence of private companies and 'lock-in' – less discussed, but equally important to consider is that technical solutions such as these are being provided by private companies which have no obligation to share their proprietary information. This means if a system was adopted and employed, it is highly unlikely that citizens – or even the PD – would have access to the internal elements of the system to try and understand how it works or to improve it if issues occur. Private companies with PDs across the country also enter them into non-disclosure agreements and other legal mechanisms to reduce what is even able to be discussed publicly about the technologies. This undercuts and is contrary to the public deliberation essential to our own shared municipal governance. Further, once a technology is chosen, there is 'lock-in' where we tend to look for improvements from the same company due to its monopoly. This means alternatives and improvements in the future will be overlooked due to previous relationships (e.g. think about how you use Zoom without question now, even though alternative video platforms with the same functionality/less privacy concerns exist – you are 'locked-in' to the first choice made).

3) Investing in the community – much like the budgetary decision in weeks prior to not invest in further funding for the PD, a decision to ban facial surveillance is a moral action which demonstrates the city's commitment to its citizens. The proactive step of banning facial surveillance frees up the opportunity for investment into our community in more tangible ways, such as greater funds for our physical and mental health services, housing support, or neighborhood investment more broadly. Facial surveillance is being touted as the 'next generation of law enforcement' but we should recognize this for what it is: a private company advertising its services in the hopes of increasing sales. We should not purchase more unnecessary products and services; we should invest in our community instead.

Adopting the ban on facial surveillance in the city not only demonstrates a moral commitment to our city and citizens, it also counters a growing trend to employ technology with the hopes of 'revolutionizing' practices when really little changes. I am asking you to support agenda item 76 and ban facial surveillance in the city completely, with no further amendments.

If you have any questions or would like any sources/data for the above points, please feel free to reach out to me.

Thank you,

Xerxes Minocher

10 Lakewood Gardens Lane, Madison, WI

From: Gregory Gelembiuk <gwgelemb@wisc.edu>
Sent: Monday, November 30, 2020 1:53 PM
To: All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject: Please support ordinance prohibiting use of face surveillance

Caution: This email was sent from an external source. Avoid unknown links and attachments.

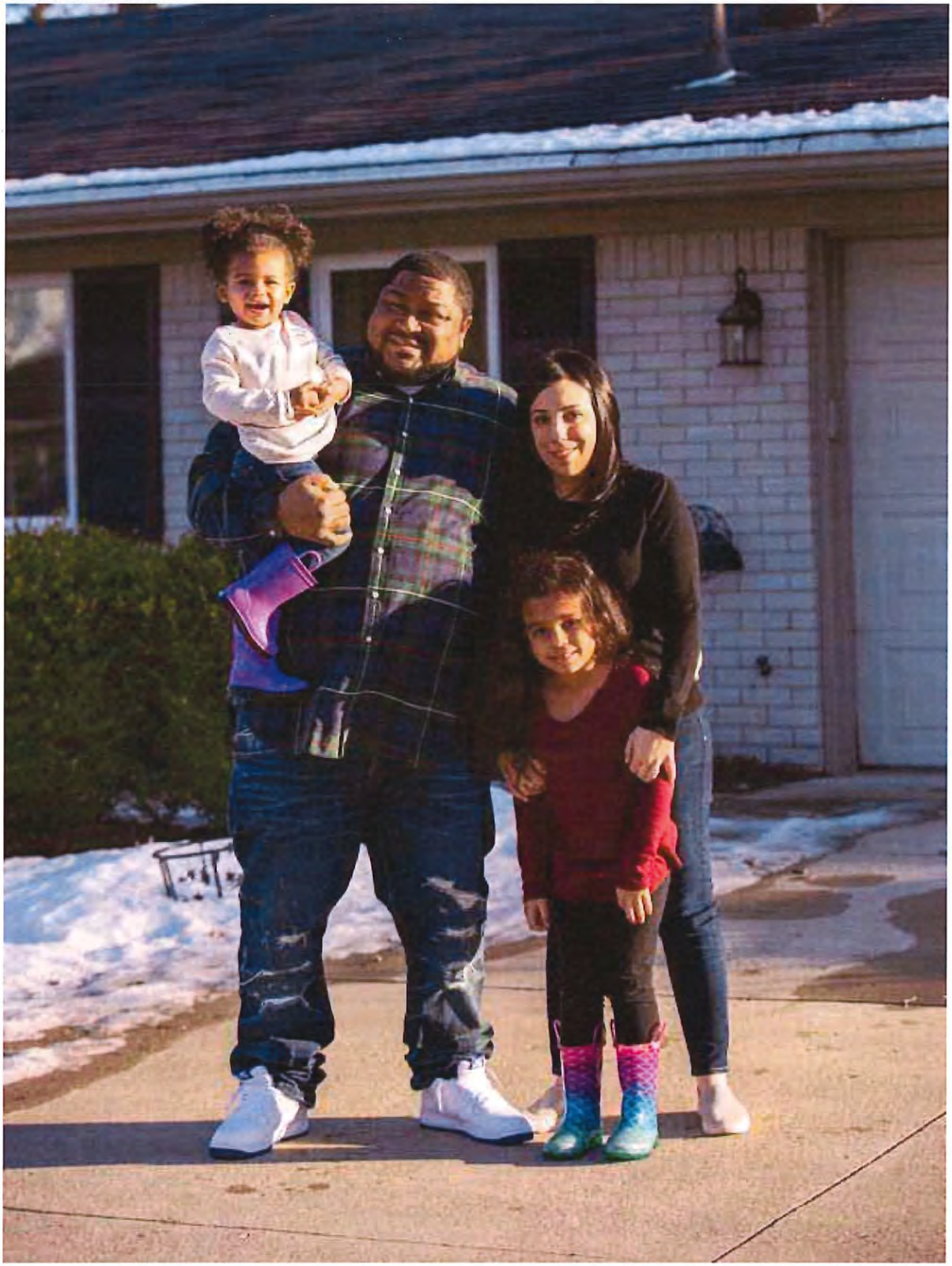
Dear Alders and Mayor,

I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

As Robert Williams, a Black Detroit resident, writes in a Washington Post article:

> I was wrongfully arrested because of facial recognition. Why are police allowed to use it?... Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed. What's worse is that, before this happened to me, I actually believed them. I thought, what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?

Robert Williams and his



family:

Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.

The ACLU states:

> We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.

Institutions such as the Georgetown Law Center on Privacy and Technology are also calling for a ban, noting that "a dramatic range of abuse and bias has surfaced". As Lindsey Barret of Georgetown Law Center writes in the publication "Ban Facial Recognition Technologies for Children – and Everyone Else":

> Clearview AI, which has been heavily criticized for its privacy violative services, has been quick to tout the use of its product in cases involving children, including investigations into child sexual exploitation. The horrendous nature of those crimes may seem to reduce the need for scruples when it comes to the harms of these technologies, when in fact the sensitivity of the circumstances makes their problems even more concerning. The false identification of a victim could be deeply traumatic, and the false identification of an ostensible perpetrator could lead to tremendously damaging consequences for the wrongly identified.

Anna Lauren Hoffmann, a professor at University of Washington Information School, writes:

> Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium.... As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.

Facial recognition software produces inaccurate and biased results.

Some people have a mistaken belief that facial recognition technology works as it's portrayed in TV shows like NCIS. Such shows are science fiction – reality is totally different.

Inaccuracy is particularly high with children and the elderly. The 2019 NIST (National Institute of Standards and Technology) Facial Recognition Vendor Test report, examining 189 facial recognition algorithms from 99 vendors (most of the industry), shows that with ideal photos (i.e., taken under the best and most uniform conditions) of two different children, the typical vendor algorithm will incorrectly conclude that they're the same child 1% of the time (making this technology largely useless for children). Moreover, for adults, when comparing two different ideal photos to verify if they're the same individual, almost all existing vendor algorithms show elevated rates of false matches for Black, Asian, and especially Native American individuals, compared to White individuals. Meanwhile, for seeking an individual's identity from an ideal photo by comparing it to a database of ideal photos of different people ("one-to-many" matching), the NIST report concludes that "low FPIR [false positive identification rate] is not attainable" (a substantial rate of false matches can't be avoided). And in such analyses, existing facial recognition software algorithms exhibit greatly elevated rates of false positives with faces of Black individuals, and especially Black women. Moreover, as one article notes of the NIST findings...

> accuracy is only possible in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the subjects are clear and unobscured. In real world deployments, accuracy rates tend to be far lower. For example, the FRVT [2019 NIST Facial Recognition Vendor Test] found that the error rate for one leading algorithm climbed from 0.1% [for middle-aged adults] when matching against high-quality mugshots to 9.3% when matching instead to pictures of individuals captured 'in the wild,' where the subject may not be looking directly at the camera or may be obscured by objects or shadows.

Thus, a 2018 study by a British nonprofit found:

> The overwhelming majority of the police's "matches" using automated facial recognition to date have been inaccurate. On average, **a staggering 95% of "matches" wrongly identified innocent people**... Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people.

Police facial recognition will disproportionately harm Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals.

Facial recognition technology constitutes a grave danger to civil liberties

Facial recognition technology infringes on a vital constitutional principle, the right to privacy, raising serious 4th amendment issues. It can permit cataloging of sensitive information and unchecked location tracking. And it can profoundly impact 1st amendment rights - endangering and chilling 1st amendment activities and press freedoms.

In their article "Facial Recognition Is the Perfect Tool for Oppression", Woodrow Hartzog (Professor of Law and Computer Science at Northeastern University School of Law) and Evan Selinger (Professor of Philosophy at Rochester Institute of Technology) note:

> facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented. It's the missing piece in an already dangerous surveillance infrastructure, built because that infrastructure benefits both

> the government and private sectors. And when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering....
>
> It's easy to think people don't have a strong privacy interest in faces because many of us routinely show them in public.... The thing is we actually do have a privacy interest in our faces, and this is because humans have historically developed the values and institutions associated with privacy protections during periods where it's been difficult to identify most people we don't know. Thanks to biological constraints, the human memory is limited; without technological augmentation, we can remember only so many faces. And thanks to population size and distribution, we'll encounter only so many people over the course of our lifetimes. These limitations create obscurity zones.

The Project On Government Oversight (POGO), a nonpartisan watchdog, has issued a report entitled "Facing the Future of Surveillance". It starkly outlines several of the severe dangers to liberty posed by facial recognition technology. Here's an excerpt:

> In last year's landmark Supreme Court decision Carpenter v. United States, the Supreme Court took on the novel risks surveillance in the digital age pose, fully embracing the right to privacy. In an opinion focused on cellphone tracking, the Court declared that "the [Fourth] Amendment seeks to secure *the privacies of life* against arbitrary power" (emphasis added), a framing that notably focuses not on certain places or types of conversation, but rather on protecting details of each person's life against an ever-watching government. Perhaps even more explicitly, the opinion of the Court in Carpenter stated that "a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance."....
>
> When the Court in Carpenter highlighted that location records "hold for many Americans *the privacies of life*" (emphasis added), it was emphasizing that Fourth Amendment privacy protections do not focus narrowly on privately owned places, but rather on people themselves, wherever they may be.... In Carpenter, the Court highlighted that "a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner," and therefore presents heightened risks to privacy. While cell phones may have become an extension of our bodies, our faces require no such metaphor; unlike cellphones, our faces are never able to be turned off, left behind, or cast aside. If our faces can be subjected to the same type of continuous surveillance as cellphones, strong limits on surveillance technology will be necessary to properly rebalance power between the government and the people....
>
> Facial recognition amplifies the concerns of upending privacy and unbalancing power between the government and its citizens in a unique and especially troubling way. The Supreme Court's key fear in both Jones and Carpenter was that in the course of tracking location, the government would unearth individuals' most sensitive activities. As Justice Sotomayor highlighted, this form of surveillance could catalog "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."... Such data could be used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to applications for background checks, to evaluations for civil service employment opportunities. Equally important is the potentially chilling effect on political and other types of participation, such as religious and community activities....
>
> Facial recognition surveillance threatens to become as powerful a method of finding and tracking individuals as are cellphone and GPS tracking. While the Supreme Court has imposed a warrant requirement for these other forms of electronic location tracking, no such limit exists for facial recognition. In time, facial recognition could become a uniquely powerful location-tracking tool because there is no "middle man" for government-managed cameras that controls access to the data; the entire surveillance system is managed and all relevant information is obtained directly by law enforcement...
>
> A necessary aspect of freedom of expression and association is group anonymity. Over six decades ago, the Supreme Court held that "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." In that case, NAACP v. Alabama, the key action at issue was the government demanding NAACP's Alabama membership list. In the digital age, no such direct action is necessary to remove the anonymity of an organization's members. A single camera outside the entrance or exit to a group's events combined with facial recognition could produce a membership list without consent or even notification. And because such identification can be done with practically no expenditure of human resources, it can be conducted on a mass scale....
>
> Facial recognition could be a tool to disrupt First Amendment-protected activities. Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and then arrest any individual with an active bench warrant. Ability to effortlessly identify any bench warrant for any petty offense could enable arbitrary action and abusive targeting, such as against selectively targeted individuals attending "events of interest," such as protests, political events, and religious ceremonies. This was

> already observed on a small scale with Geofeedia—a social media-monitoring company—which admitted that Baltimore police used the service during protests to "run social media photos through facial recognition technology" to find individuals with "outstanding warrants and arrest them directly from the crowd," with the goal of targeting individuals who were protesting. Given the number of bench warrants for petty offenses that some municipalities maintain, it is entirely possible that facial recognition could become an "arrest-at-will" authority used to disrupt such activities on a broad basis....
>
> Modern surveillance powers force journalists to take extra precautions, such as leaving cell phones and other electronic devices with built in GPS at home. But facial recognition can be used not just to catalog activities, but also interactions. If it becomes a tool to pinpoint how individuals interact and meet with journalists, it could present significant roadblocks for journalists seeking to speak to sources and whistleblowers while preserving anonymity.

Face surveillance technology imposes yet another serious problem. As the ACLU notes in a letter to Oakland elected officials (and the same would apply for Madison):

> any facial recognition system would require a massive sensitive database featuring the sensitive face prints of Oakland [Madison] residents ***without their consent***. To attempt to identify or track a person by their biometric features, a facial recognition system requires the biometric information of a substantial number of individuals to match against. If such a system were built in Oakland [Madison], individual Oaklanders [Madison residents] would not have the opportunity to consent to the exploitation of their sensitive biometric information or the use of such technology against them. The information in these huge matching databases may become attractive targets for malicious actors and the target of exploitation attempts by other government agencies, such as ICE. And a database of sensitive biometric information is a liability and vulnerable to breach: just this month, we learned that face images of American travelers held by the Customs and Border Protection were hacked and leaked onto the internet.

Face surveillance is a menace disguised as a gift. Its implementation threatens to leave us all less free. Please support a strict ban on the use of this violative technology.

Sincerely,
Dr. Gregory Gelembiuk

Veldran, Lisa

From:	Elizabeth Falkos <bdjfalkos@hotmail.com>
Sent:	Monday, November 30, 2020 2:58 PM
To:	All Alders; Mayor; Attorney
Subject:	Facial Recognition Technology

Dear Alders and Mayor Conway-Rhodes:

I urge you to fully consider the important ways the MPD is using FRT at this time and the options for future use to keep our community safe. A rushed vote to limit the MPD from using it at the Council Meeting tomorrow will not serve our city well. Other police departments are using it wisely and have reasonable plans in place. We need to look at the research of how it's being used elsewhere, fully understand the safeguards the MPD already has in place, and stay leading edge in having the latest technology for saving victims and solving crimes.

I ask you to **OPPOSE Item #76** Establishing a Ban on the Use of Face Surveillance Technology.

I understand concerns about balancing individual privacy with the advantages that FRT can bring to public safety and security. The development of some common procedures and implementation guidelines for all City departments should be considered. This will help to assure Madison residents that the technology is being used appropriately.

Please view: "Facial Recognition Technology: Balancing Safety and Privacy" from the Wisconsin Legislative Reference Bureau at:

https://docs.legis.wisconsin.gov/misc/lrb/wisconsin_policy_project/facial_recognition_privacy_3_4.pdf

Thank you, Beth Falkos
6218 Countryside Ln
Madison, WI 53705

Veldran, Lisa

From:	Stacey Williams <swilliams6681@gmail.com>
Sent:	Monday, November 30, 2020 3:33 PM
To:	All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject:	Please support ban on facial recognition

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders and Mayor,

I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

As Robert Williams, a Black Detroit resident, writes in a Washington Post article:

> I was wrongfully arrested because of facial recognition. Why are police allowed to use it?... Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed. What's worse is that, before this happened to me, I actually believed them. I thought, what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?

Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.
The ACLU states:

> We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.

Institutions such as the Georgetown Law Center on Privacy and Technology are also calling for a ban, noting that "a dramatic range of abuse and bias has surfaced". As Lindsey Barret of Georgetown Law Center writes in the publication "Ban Facial Recognition Technologies for Children – and Everyone Else":

> Clearview AI, which has been heavily criticized for its privacy violative services, has been quick to tout the use of its product in cases involving children, including investigations into child sexual exploitation. The horrendous nature of those crimes may seem to reduce the need for scruples when it comes to the harms of these technologies, when in fact the sensitivity of the circumstances makes their problems even more concerning. The false identification of a victim could be deeply traumatic, and the false identification of an ostensible perpetrator could lead to tremendously damaging consequences for the wrongly identified.

Anna Lauren Hoffmann, a professor at University of Washington Information School, writes:

> Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium.... As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.

Facial recognition software produces inaccurate and biased results.
Some people have a mistaken belief that facial recognition technology works as it's portrayed in TV shows like NCIS. Such shows are science fiction – reality is totally different.
Inaccuracy is particularly high with children and the elderly. The 2019 NIST (National Institute of Standards and Technology) report shows that if you use ideal photos (i.e., the best possible conditions) for both a test photo of a child and a database of photos of different children, the typical vendor algorithm will incorrectly call 1% of all photos in the database a match (making this technology close to useless for children). There's also racial bias - existing facial recognition software exhibit greatly elevated error rates with faces of Black folks, and especially Black women. Moreover, as one article notes of the NIST findings...

> accuracy is only possible in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the subjects are clear and unobscured. In real world deployments, accuracy rates tend to be far lower. For example, the FRVT [2019 NIST Facial Recognition Vendor Test] found that the error rate for one leading algorithm climbed from 0.1% [for middle-aged adults] when matching against high-quality mugshots to 9.3% when matching instead to pictures of individuals captured 'in the wild,' where the subject may not be looking directly at the camera or may be obscured by objects or shadows.

Thus, a 2018 study by a British nonprofit found:

> The overwhelming majority of the police's "matches" using automated facial recognition to date have been inaccurate. **On average, a staggering 95% of "matches" wrongly identified innocent people**... Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people.

Police face recognition will disproportionately harm Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals.
Facial recognition technology constitutes a grave danger to civil liberties
Facial recognition technology infringes on a vital constitutional principle, the right to privacy, raising serious 4th amendment issues. It can permit cataloging of sensitive information and unchecked location tracking. And it can profoundly impact 1st amendment rights - endangering and chilling 1st amendment activities and press freedoms.
In their article "Facial Recognition Is the Perfect Tool for Oppression", Woodrow Hartzog (Professor of Law and Computer Science at Northeastern University School of Law) and Evan Selinger (Professor of Philosophy at Rochester Institute of Technology) note:

> facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented. It's the missing piece in an already dangerous surveillance infrastructure, built because that infrastructure benefits both the government and private sectors. And when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering....
>
> It's easy to think people don't have a strong privacy interest in faces because many of us routinely show them in public.... The thing is we actually do have a privacy interest in our faces, and this is because humans have historically developed the values and institutions associated with privacy protections during periods where it's been difficult to identify most people we don't know. Thanks to biological constraints, the human memory is limited; without technological augmentation, we can remember only so many faces. And thanks to population size and distribution, we'll encounter only so many people over the course of our lifetimes. These limitations create obscurity zones.

The Project On Government Oversight (POGO), a nonpartisan watchdog, has issued a report entitled "Facing the Future of Surveillance". It starkly outlines several of the severe dangers to liberty posed by facial recognition technology. Here's an excerpt:

> In last year's landmark Supreme Court decision Carpenter v. United States, the Supreme Court took on the novel risks surveillance in the digital age pose, fully embracing the right to privacy. In an opinion focused on cellphone tracking, the Court declared that "the [Fourth] Amendment seeks to secure ***the privacies of life*** against arbitrary power" (emphasis added), a framing that notably focuses not on certain places or types of conversation, but rather on protecting details of each person's life against an ever-

watching government. Perhaps even more explicitly, the opinion of the Court in Carpenter stated that “a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance.”,,,,

When the Court in Carpenter highlighted that location records “hold for many Americans **the privacies of life**” (emphasis added), it was emphasizing that Fourth Amendment privacy protections do not focus narrowly on privately owned places, but rather on people themselves, wherever they may be.... In Carpenter, the Court highlighted that “a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner,” and therefore presents heightened risks to privacy. While cell phones may have become an extension of our bodies, our faces require no such metaphor; unlike cellphones, our faces are never able to be turned off, left behind, or cast aside. If our faces can be subjected to the same type of continuous surveillance as cellphones, strong limits on surveillance technology will be necessary to properly rebalance power between the government and the people....

Facial recognition amplifies the concerns of upending privacy and unbalancing power between the government and its citizens in a unique and especially troubling way. The Supreme Court’s key fear in both Jones and Carpenter was that in the course of tracking location, the government would unearth individuals’ most sensitive activities. As Justice Sotomayor highlighted, this form of surveillance could catalog “trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.”... Such data could be used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to applications for background checks, to evaluations for civil service employment opportunities. Equally important is the potentially chilling effect on political and other types of participation, such as religious and community activities....

Facial recognition surveillance threatens to become as powerful a method of finding and tracking individuals as are cellphone and GPS tracking. While the Supreme Court has imposed a warrant requirement for these other forms of electronic location tracking, no such limit exists for facial recognition. In time, facial recognition could become a uniquely powerful location-tracking tool because there is no “middle man” for government-managed cameras that controls access to the data; the entire surveillance system is managed and all relevant information is obtained directly by law enforcement...

A necessary aspect of freedom of expression and association is group anonymity. Over six decades ago, the Supreme Court held that “Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.” In that case, NAACP v. Alabama, the key action at issue was the government demanding NAACP’s Alabama membership list. In the digital age, no such direct action is necessary to remove the anonymity of an organization’s members. A single camera outside the entrance or exit to a group’s events combined with facial recognition could produce a membership list without consent or even notification. And because such identification can be done with practically no expenditure of human resources, it can be conducted on a mass scale....

Facial recognition could be a tool to disrupt First Amendment-protected activities. Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and then arrest any individual with an active bench warrant. Ability to effortlessly identify any bench warrant for any petty offense could enable arbitrary action and abusive targeting, such as against selectively targeted individuals attending “events of interest,” such as protests, political events, and religious ceremonies. This was already observed on a small scale with Geofeedia—a social media-monitoring company—which admitted that Baltimore police used the service during protests to “run social media photos through facial recognition technology” to find individuals with “outstanding warrants and arrest them directly from the crowd,” with the goal of targeting individuals who were protesting. Given the number of bench warrants for petty offenses that some municipalities maintain, it is entirely possible that facial recognition could become an “arrest-at-will” authority used to disrupt such activities on a broad basis....

> Modern surveillance powers force journalists to take extra precautions, such as leaving cell phones and other electronic devices with built in GPS at home. But facial recognition can be used not just to catalog activities, but also interactions. If it becomes a tool to pinpoint how individuals interact and meet with journalists, it could present significant roadblocks for journalists seeking to speak to sources and whistleblowers while preserving anonymity.

Face surveillance is a menace disguised as a gift. Its implementation threatens to leave us all less free. Please support a strict ban on the use of this violative technology.

Sincerely,
Stacey Williams
Madison resident - Emerson East

Veldran, Lisa

From:	Carissa Wegner <carissa396@gmail.com>
Sent:	Monday, November 30, 2020 4:40 PM
To:	All Alders
Subject:	Please oppose item 62413 (ban on facial recognition technology)

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Hello Alders,

I'm writing to ask you to consider opposing agenda item 62413 tomorrow night. I am very concerned about the safety of children using the internet (as they increasingly have to) , and would like the MPD to be allowed to use all technology to protect them.
Please do not ban Facial Recognition Technology. Please work with MPD to help and protect vulnerable kids.

Thanks so much for considering,
Carissa Wegner
Piper Drive
Madison

From:	e2reichel@att.net
Sent:	Monday, November 30, 2020 8:45 PM
To:	Mayor
Cc:	mbottarie@cityofmadison.com; All Alders; e2reichel@att.net
Subject:	Item 76 (Agenda Item 62413), Item 77 (Agenda Item 62908)

Caution: This email was sent from an external source. Avoid unknown links and attachments.

We have hired our Police Department to fight crime. Please get out of their way and let them fight it as they are trained to do it. All of these proposed rule changes are making it impossible for them to do a respectful job of protecting us. Think back! We have much to be thankful for over the past many years for their excellent work of keeping our city safe.

Let us stop the criminals from taking over our society.

Thank God we have a wonderful department. This is the City we love. Letting down our guard and letting criminals off will ruin our city.

People who behave themselves are not against using the latest technologies to catch criminals and those who are not interested in following our desired levels of behavior.

Facial recognition is needed. The criminals are using all the latest technologies they can find!

Table this Ordinance so this important issue can be properly conducted.

Earl H. Reichel

Veldran, Lisa

From: Quinn Crossley <qncrossley@gmail.com>
Sent: Monday, November 30, 2020 8:46 PM
To: All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject: Please support the ban on facial recognition technology

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Hi Alders and Mayor Rhodes-Conway,
My name is Quinn Crossley and I'm a resident of Madison, living on the isthmus at 26 S Bedford St #410, Madison, WI 53703.

I'm writing in support of the proposed ban on facial recognition technology that is on the agenda for tomorrow's city council meeting.

Increasing surveillance in our city will make our lives worse, not better. Allowing MPD to use facial recognition is an invasion of our privacy and it will lead to disproportionate harm and violence in our BIPOC communities.

Studies have repeatedly demonstrated that facial recognition technology is biased - both in the technology itself and in the way that it is applied. Additionally, as a tech worker, I have personally witnessed time and time again how rampant inequity in the tech industry has led to new technology that further cements existing systemic injustices.

I urge you all to support the ban on facial recognition technology as it is currently written, without any new watered down language. In order to protect our community, it is critical to pass a strong measure that bans the use of this technology before it is fully implemented. Please take this step to make Madison a safer and more inclusive city.

Thank you,
Quinn Crossley
26 S Bedford St #410, Madison, WI 53703.

From: Bianca Tomasini <brtj2457@gmail.com>
Sent: Monday, November 30, 2020 9:48 PM
To: All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject: Support for agenda item 76 to ban use of facial recognition technology

Dear Alders, Mayor and Staff,
I am in support of banning the use of facial recognition technology by MPD.
The level of misuse and potential abuse, together with the intrinsic flaws in algorithms that clearly misidentify people of color compared to white males, make the use of this technology very dangerous policy that puts us farther away from justice and equity. That's what we want, right? We want a just and equitable Madison asap.

https://www.itpro.com/data-protection/31117/facial-recognition-technology-is-dangerously-inaccurate

One can imagine that supporters of the use of face recognition by police at this time are more likely to be interested in surveilling protestors, for instance. In their article "Facial Recognition Is the Perfect Tool for Oppression", Woodrow Hartzog (Professor of Law and Computer Science at Northeastern University School of Law) and Evan Selinger (Professor of Philosophy at Rochester Institute of Technology) note:
"facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented." Over six decades ago, the Supreme Court held that "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."

Does Madison government want to facilitate infringement of 1st and 4th amendment rights? I hope the answer is no.
Instead, take a look at this ordinance passed in Boston that bans facial surveillance technology for the very reason that it is racially inequitably and unjust:
https://www.dataguidance.com/.../docket_0683 - boston...
We need to ban facial recognition use by MPD and draft an ordinance similar to that used in Boston.

Why do we have to keep battling for racial justice and equity at every turn? Madison representatives should stand for this already, simply because it's the moral thing to do - ban use facial surveillance technology.

Sincerely,

Bianca Tomasini, 4926 Odana Rd,Madison, 53711

District 10

"a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance.",,,,

from last year's landmark Supreme Court decision Carpenter v. United States,

From: Robert Meyer <rrm.rrm@gmail.com>
Sent: Monday, November 30, 2020 10:35 PM
To: All Alders; Mayor
Subject: Facial recognition is an essential tool, don't ban it

Caution: This email was sent from an external source. Avoid unknown links and attachments.

We have enjoyed living in Madison since 1972, but recent actions by the city government are calling into question how much longer we will want to reside here. We see an inclination on the part of city government to follow bad examples that have been set elsewhere in terms of public safety and police practice. The most recent example is the consideration of an ordinance to ban facial recognition. We see no sound arguments to support such an ordinance, but instead regard it as another attempt to prop up on imaginary legs the false narrative that the police rather than criminals are wrongdoers. Passing this ordinance will only serve to make criminals bolder and Madison even less safe.

Sincerely,

Barbara and Robert Meyer

730 Wedgewood Way

Madison 53711

From: Michelle Kaiser <kaiserm13@gmail.com>
Sent: Monday, November 30, 2020 10:51 PM
To: All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject: Ordinance to ban use of facial recognition technology by City of Madison

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders and Mayor,

I am writing to encourage you to support the proposed ordinance to prohibit use of face surveillance technology by City departments. Please do not weaken this ordinance. Facial recognition systems are dangerous to civil liberties. We need a strict prohibition on its use.

Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. This is a flawed system!

Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.

This system can lead to wrongful arrests, use of force, abuse, bias and grave harm. It also poses a threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.

Some may feel that this technology could help in cases involving children, including investigations into child sexual exploitation. However, the 2019 National Institute of Standards and Technology report showed that if you use ideal photos (i.e., the best possible conditions) for both a test photo of a child and a database of photos of different children, the typical vendor algorithm will incorrectly call 1% of all photos in the database a match (making this technology close to useless for children). There's also racial bias - existing facial recognition software exhibit greatly elevated error rates with faces of Black folks, and especially Black women.

A 2018 study by a British nonprofit found: The overwhelming majority of the police's "matches" using automated facial recognition to date have been inaccurate. On average, a staggering 95% of "matches" wrongly identified innocent people… Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people.

Police face recognition disproportionately harms Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals.

Facial recognition technology constitutes a grave danger to civil liberties. Facial recognition technology infringes on a vital constitutional principle, the right to privacy, raising serious 4th amendment issues. It can permit cataloging of sensitive information and unchecked location tracking. And it can profoundly impact 1st amendment rights - endangering and chilling 1st amendment activities and press freedoms.

We already have a dangerous surveillance infrastructure, built because that infrastructure benefits both the government and private sectors. And when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering...

In last year's landmark Supreme Court decision Carpenter v. United States, the Supreme Court took on the novel risks surveillance in the digital age pose, fully embracing the right to privacy. In an opinion focused on cellphone tracking, the Court declared that "the [Fourth] Amendment seeks to secure the privacies of life against arbitrary power" (emphasis added), a framing that notably focuses not on certain places or types of conversation, but rather on protecting details of each person's life against an ever-watching government. Perhaps even more explicitly, the opinion of the Court in Carpenter stated that "a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance.",,,, When the Court in Carpenter highlighted that location records "hold for many Americans the privacies of life" (emphasis added), it was emphasizing that Fourth Amendment privacy protections do not focus narrowly on privately owned places, but rather on people themselves, wherever they may be.... In Carpenter, the Court highlighted that "a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner," and therefore presents heightened risks to privacy. While cell phones may have become an extension of our bodies, our faces require no such metaphor; unlike cellphones, our faces are never able to be turned off, left behind, or cast aside. If our faces can be subjected to the same type of continuous surveillance as cellphones, strong limits on surveillance technology will be necessary to properly rebalance power between the government and the people....

Facial recognition amplifies the concerns of upending privacy and unbalancing power between the government and its citizens in a unique and especially troubling way. The Supreme Court's key fear in both Jones and Carpenter was that in the course of tracking location, the government would unearth individuals' most sensitive activities. As Justice Sotomayor highlighted, this form of surveillance could catalog "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."... Such data could be used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to applications for background checks, to evaluations for civil service employment opportunities. Equally important is the potentially chilling effect on political and other types of participation, such as religious and community activities....

Facial recognition surveillance threatens to become as powerful a method of finding and tracking individuals as are cellphone and GPS tracking. While the Supreme Court has imposed a warrant requirement for these other forms of electronic location tracking, no such limit exists for facial recognition. In time, facial recognition could become a uniquely powerful location-tracking tool because there is no "middle man" for government-managed cameras that controls access to the data; the entire surveillance system is managed and all relevant information is obtained directly by law enforcement...

A necessary aspect of freedom of expression and association is group anonymity. Over six decades ago, the Supreme Court held that "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." In that case, NAACP v. Alabama, the key action at issue was the government demanding NAACP's Alabama membership list. In the digital age, no such direct action is necessary to remove the anonymity of an organization's members. A single camera outside the entrance or exit to a group's events combined with facial recognition could produce a membership list without consent or even notification. And because such identification can be done with practically no expenditure of human resources, it can be conducted on a mass scale....

Facial recognition could be a tool to disrupt First Amendment-protected activities. Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and then arrest any individual with an active bench warrant. Ability to effortlessly identify any bench warrant for any petty offense could enable arbitrary action and abusive targeting, such as against selectively targeted individuals attending "events of interest," such as protests, political events, and religious ceremonies. Given the number of bench warrants for petty offenses that some municipalities maintain, it is entirely possible that facial recognition could become an "arrest-at-will" authority used to disrupt such activities on a broad basis....

Modern surveillance powers force journalists to take extra precautions, such as leaving cell phones and other electronic devices with built in GPS at home. But facial recognition can be used not just to catalog activities, but also interactions. If it becomes a tool to pinpoint how individuals interact and meet with journalists, it could present significant roadblocks for journalists seeking to speak to sources and whistleblowers while preserving anonymity.

Face surveillance is a menace disguised as a gift. Its implementation threatens to leave us all less free. 2020 has shown that racism and biases are still real and an issue. Please do not add the threats this technology can impose to an already broken law enforcement system.

Please support a strict ban on the use of this violative technology. Thank you for your time.

Sincerely,
Michelle Kaiser
Madison, WI

Veldran, Lisa

From:	Alice Herman <alice.herman22@gmail.com>
Sent:	Monday, November 30, 2020 11:19 PM
To:	All Alders
Cc:	Rummel, Marsha
Subject:	Please support the Ban on the Use of Face Surveillance Technology

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear alders,

I am a resident of District 6, writing to urge all alders to support the proposal to ban the use of facial recognition technology by city departments, including the Madison Police Department.

Facial recognition technology is notoriously unreliable, particularly in assessing the faces of people who aren't white.

A 2018 study by the ACLU illustrates the problem: when the organization tested Amazon's facial recognition software on the US House of Representatives, the software identified 28 members of congress (disproportionately, congresspeople of color), including Rep. John Lewis, as people from a database of publicly available arrest photos. In short, the software wasn't smart enough to tell many members of US congress from random mugshots.

Using facial recognition technology risks the miscarriage of justice, particularly for Black and brown Madisonians—an unacceptable risk.

Thanks for considering taking up Ald. Presigiacomo's proposed ban on this technology.

Sincerely,
Alice Herman

Veldran, Lisa

From: Gisela Wilson <giselawilson@gmail.com>
Sent: Tuesday, December 01, 2020 12:11 AM
To: All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject: Agenda Item #76 — In Support of Facial Recognition Ban

Caution: This email was sent from an external source. Avoid unknown links and attachments.

allalders@cityofmadison.com
srhodes-conway@cityofmadison.com
mbottari@cityofmadison.com

30 November 2020

Re: Agenda Item #76 — In Support of Facial Recognition Ban

Dear Madison Alders and and Mayor Rhodes-Conway,

I am writing **in strong support of the ban on use of facial surveillance technology** by all city departments, including the MPD. I would prefer county law enforcement to be included in the ban as well. I also am strongly against watering it down with amendments.

For the reasons stated in more detail below, the ban should also (a) prevent MPD or the city contracting with third party vendors to obtain the results of facial recognition searches, (b) prevent the use of this technology to surveil protests, and (c) prevent the incorporation of facial recognition with body cams. In fact, that law enforcement officials have suggested they will only use facial recognition technology to increase possible leads (that are then verified using other investigative methods) is belied by consideration of combining facial recognition technology with body cams -- circumstances in which machine "matches" will be used in the immediate moment. **I ask all Alders and the Mayor to support a strict ban on facial surveillance technology in full.**

Facial recognition technology is more than a waste of tax dollars. The technology is extremely problematic because of its current inaccuracies and biases. However, **facial recognition technology would also be extremely problematic even if it were 100% accurate. Possible benefits of this new technology are far outweighed by its many harms. Facial Recognition is morally objectionable :** (a) the databases it relies on are obtained via illegal search and seizure and, as such, is a clear violation of the 4th Amendment; (b) use of the technology by either public and private enterprise is destructive to our right to privacy and freedom to assemble. Facial recognition is an existential threat. These points are elaborated below:

A) **Facial Recognition Technology's Inaccuracies and Biases** : Currently, facial recognition technology is highly error prone, with both high false positive and false negative rates. It was only a few years ago that state-of-art machine/deep learning algorithms misidentified Queen Elizabeth as a shower cap and labelled people of color as apes. Even when limiting the identification task to faces, Amazon's facial recognition system recently mis-identified over two dozen congressional representatives as criminals[1]. **Machine learning systems largely "learn" on their own, so the decision trees that contribute to errors in final output cannot be traced and corrected.**

Sources of error due to design of facial recognition technology include (a) the datasets that are used to train (teach) the machine learning system; (b) the choice of which features are most critical for a "match"; (c) variations in lighting, resolution, angle and distance. For examples of how these biases affect results, databases and machine learning systems based on mugshots will overrepresent people of color due to the racial bias inherent in the criminal justice system. Further, these databases assume criminality even though the photos are of people who haven't been convicted of any crime. In contrast, databases and machine learning based on driver's license photos will be majority white and therefore will under-specify features associated with people of color, not to mention children. Finally, databases constructed from publicly available photos (e.g., CCTV or Facebook) will exhibit more bias resulting from differences in quality, lighting or other contextual cues. Similarities in hairstyles, clothing, and make-up also can cause mis-matches[2].

In addition, there are also **sources of error due to use,** including (d) automation bias, (e) confirmation bias, and (f) reckless use. Automation bias is the tendency to treat a machine's output as fact, not understanding the potential sources of error outlined above or variations in the types of bias in systems with differences in design. Confirmation bias is the tendency to believe any output provided by the system that supports an already held view or suspicion, regardless of the credibility of the source. Numerous scientists and human rights advocates have indicated facial recognition technology currently lacks credibility.

Given the high error rate of facial recognition technology and the repercussions of a mistake, all use of facial recognition technology is reckless use at this time. On these grounds, fourteen cities including San Francisco and Boston have already banned its use. Forty informed groups have called for a moratorium[3]. Why invest in a technology that isn't reliable, can cause tremendous harm, and which further exacerbates existing societal biases ?

Imagine the semblance you were matched to originated from a mugshot database. And that the people who did the matching were police immediately swarming and surrounding you with tasers and/or guns drawn. Imagine losing your job or the goodwill of your stranger neighbors due to the hullabaloo. Imagine being thrown in jail without the opportunity to inquire or prove they had the wrong person[4]. Police are intuitively going to believe the results of technology that is there to help them, especially when it confirms their already existing biases. Even without facial recognition software, this is already a problem: I clearly remember MPD pulling over and surrounding with guns drawn, a Black woman driving her car home this summer. She had reported her car stolen, and then reported it found before driving it home. Maybe a clerical time delay was at fault or another type of glitch. **The more we rely on databases and software the greater the opportunities for life-altering glitches. The time scale on which police act and the seriousness of potential consequences makes facial recognition an extremely UNWISE choice for Law Enforcement.**

A 2019 NIST (National Institute of Standards and Technology) study evaluating the error rates of different facial recognition systems designed in the U.S. found up to a 100-fold difference in mismatch errors for Black, Asian-American, and Native American adults . False positive rates were also much higher for women, elderly and children[5]. Other studies have found mis-match rates as high as 80% and 95%.

As sympathetic as all of us must be towards cases of missing or trafficked children, the resulting trauma and disruption of mis-identified children and parents is not worth the risk of using facial recognition technology, especially since children are among those showing high false positive rates. "Good intentions are not enough"[6].

B) **Problems created by facial recognition even assuming 100% accuracy** . Some members of the public, including the MPD, may argue against the ban on the basis of a "Nothing To Hide" rationale — a rationale that has been soundly debunked for years[7]. The obvious intrusions of data mining and potential for hacking has only grown in the intervening time. Although facial recognition is only one part of the data puzzle, the use of facial recognition by law enforcement carries the most severe immediate repercussions. Facial surveillance is an unwarranted invasion of privacy with no probable cause. The benefits to police are minor compared to the existential cost to everyone. "The problem with the nothing-to-hide argument is the underlying assumption that privacy is about hiding bad things".

Reasons " *Nothing-To-Hide* " is garbage —

1) Denial of Due Process and Increasing Imbalances in Power: Law enforcement (and the State) already have much more information about any specific individual than individuals have about them without adding facial recognition into the mix. Moreover, police are protected by qualified immunity, a powerful union, and the typically unquestioned authority our society has given the police. Facial recognition technology increases the power imbalance and puts already vulnerable groups at even higher risk.

2) Lack of ownership and understanding of origins: Facial recognition relies on databases the police do not own and the security of those databases will increasingly be vulnerable as data is passed through an increasing number of hands, including creators, data mining, data storage, and data marketing corporations and end users. The problems increase exponentially as a function of hacking, alteration, and deep fakes. Photos can be tagged as "of interest", uprated or down-rated not only by law enforcement, but also by the owners of the databases for a variety of reasons that have little to do with criminal activity[8].

3) Exclusion : "people are prevented from having knowledge about how information about them is being used, and when they are barred from accessing and correcting errors in that data"[9].

4) Distortion of Context : While mugshots and driver's license photos are some of the most used for facial recognition databases, photos from other sources also abound with contextual problems. For example, consider an average person going shopping or to the post office captured on drone footage of a protest. Or on CCTV footage exiting the subway alongside someone on a watchlist. Alternatively, consider the difference in the nature of photos available for an orphan versus a member of a large extended family. Or consider that contextual cues in a photo might imply different things in a law enforcement context versus the actual events at which they were taken. Consider that over-policed BIPOC communities are captured by more surveillance technology than whites and that the wealth of surroundings, or more precisely lack-thereof, is implicitly associated with criminality.

5) Aggregation : "emerges from the fusion of small bits of seemingly innocuous

data" . The entire data landscape is a distortion of data points 10 (and photos) collected by businesses with self-interests other than an accurate representation of an individual, that person's character and life. Data and photos taken out of context create anomalous errors and artifacts that can be impossible for any given individual to track down.

8) Nefarious actors : Once databases exist, there is little to stop their use by stalkers and other nefarious actors, whether in law enforcement or not. People do change, whereas data can be stored forever. As a general rule, **every increase in information technology and every increase in the market forces for the use of a technology increases the 'surface area' of vulnerability (or attack surface) to an extent the human mind isn't readily able to keep up with . What's worse, corporations are increasingly washing their hands of their responsibility for the risks of their creations.** Very recently, multiple hospitals have been frozen out of their patient databases, their doctors and patients essentially held for ransom[11].

10) There is no clear legal or regulatory framework : Data mining is the wild wild West in the middle of a gold or oil rush. We are only beginning to understand its harms. **Our laws and regulatory frameworks are decades behind.**

(11) The existential threat mentioned at the beginning of this letter : As Anna Lauren Hoffmann observes[12], "Privacy is not a horror movie, most privacy problems don't result in dead bodies, and demanding evidence of palpable harms will be difficult in many cases." Without question, however, law enforcement is a context in which the palpable harms of facial recognition could result in a horror movie and dead bodies in real life.

In sum, no matter what law enforcement will try to assure you of a) Police and officials usually have little understanding of the biases and assumptions of the databases and machine/deep learning algorithms used to make identifications; b) Police and officials cannot guarantee the validity and security of the information. As a scientist, it is my firm conclusion that the existence and use of facial recognition technology offers little improvement in solving crime, is at least as likely to create more victims, and dramatically increases the "surface area" of vulnerability (or attack surface) beyond what human minds can cope with.

"As a constitutional principle embodied in the Fourth Amendment's protection from "unreasonable searches and seizures," privacy is meant to do more than create legal walls that mirror physical ones, and is not limited to situations where we are inside our own houses[13]." As the Supreme Court has recognized, the concept of privacy needs to include a "privacy of life" that allows us freedom of association in public spaces and allows us to lose ourselves in the anonymity of a crowd[14].

"Facial recognition is not a benign extension of existing surveillance practices— it's rocket fuel. We should reject anything less than a moratorium."[15] In short, Madison, if wanting to preserve the sanity of society, democracy, free speech, privacy and individual civil rights, should ban facial recognition technology, too.

Sincerely,

Gisela Wilson, PhD

[1] Facial Recognition and Equity (with Matt Cagle)

https://digitalcommons.law.scu.edu/htli_alsocialimpact/1/?fbclid=IwAR0qLwMQ2T-fW9emUT5bvJMzS-3cl6PRtBrtD2a9is3YVTeqhgp3tb17AS0

[2] Anna Lauren Hoffmann, "The privacy risks of unchecked facial-recognition technology", https://static1.squarespace.com/static/5b8ab61f697a983fd6b04c38/t/5ca3ddcb15fcc0a59411ff30/1554243020037/HoffmannSeattleTimesFaceRecOpEd.pdf

[3] Angela Chen, "40 groups have called for a US moratorium on facial recognition technology" , https://www.technologyreview.com/2020/01/27/276067/facial-recognition-clearview-ai-epic-privacy-moratorium-surveillance/ ; Letter - https://epic.org/privacy/facerecognition/PCLOB-Letter-FRT-Suspension.pdf

[4] Read the account of Robert Williams, a Black resident of Detroit, as a example of the consequences of a false match; https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/

[5] https://crosscut.com/2020/01/technology-vs-privacy-washington-looks-regulate-facialrecognition-tools-2020; https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-agesex-face-recognition-software ;
https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[6] https://crosscut.com/2020/01/technology-vs-privacy-washington-looks-regulate-facialrecognition-tools-2020

[7] Daniel J. Solove, "Why Privacy Matters Even if You Have 'Nothing to Hide'" http://www.woldww.net/classes/Information_Ethics/Solove-ChronicleArticle-NothingToHide.pdf

[8] Kashmir Hill, "The Secretive Company that Might End Privacy as We Know It" https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[9] Daniel J. Solove, "Why Privacy Matters Even if You Have 'Nothing to Hide'" http://www.woldww.net/classes/Information_Ethics/Solove-ChronicleArticle-NothingToHide.pdf

[10] ibid.

[11] Ellen Barry and Nicole Perlroth, "Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack";
https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html

[12] Anna Lauren Hoffmann, "The privacy risks of unchecked facial-recognition technology" https://static1.squarespace.com/static/5b8ab61f697a983fd6b04c38/t/5ca3ddcb15fcc0a59411ff30/1554243020037/HoffmannSeattleTimesFaceRecOpEd.pdf

[13] https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/;*Carpenter v. United States*, 585 U.S. ____ (2018)

[14] ibid.

[15] Anna Lauren Hoffmann, "The privacy risks of unchecked facial-recognition technology" https://static1.squarespace.com/static/5b8ab61f697a983fd6b04c38/t/5ca3ddcb15fcc0

a59411ff30/1554243020037/HoffmannSeattleTimesFaceRecOpEd.pdf

From: Gisela Wilson <giselawilson@gmail.com>
Sent: Tuesday, December 01, 2020 12:16 AM
To: All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject: Agenda Item #76 — In Support of Facial Recognition Ban (corrected, with address)

Caution: This email was sent from an external source. Avoid unknown links and attachments.

allalders@cityofmadison.com
srhodes-conway@cityofmadison.com
mbottari@cityofmadison.com

30 November 2020

Re: Agenda Item #76 — In Support of Facial Recognition Ban

Dear Madison Alders and and Mayor Rhodes-Conway,

I am writing **in strong support of the ban on use of facial surveillance technology** by all city departments, including the MPD. I would prefer county law enforcement to be included in the ban as well. I also am strongly against watering it down with amendments.

For the reasons stated in more detail below, the ban should also (a) prevent MPD or the city contracting with third party vendors to obtain the results of facial recognition searches, (b) prevent the use of this technology to surveil protests, and (c) prevent the incorporation of facial recognition with body cams. In fact, that law enforcement officials have suggested they will only use facial recognition technology to increase possible leads (that are then verified using other investigative methods) is belied by consideration of combining facial recognition technology with body cams -- circumstances in which machine "matches" will be used in the immediate moment. **I ask all Alders and the Mayor to support a strict ban on facial surveillance technology in full.**

Facial recognition technology is more than a waste of tax dollars. The technology is extremely problematic because of its current inaccuracies and biases. However, **facial recognition technology would also be extremely problematic even if it were 100% accurate. Possible benefits of this new technology are far outweighed by its many harms. Facial Recognition is morally objectionable :** (a) the databases it relies on are obtained via illegal search and seizure and, as such, is a clear violation of the 4th Amendment; (b) use of the technology by either public and private enterprise is destructive to our right to privacy and freedom to assemble. Facial recognition is an existential threat. These points are elaborated below:

A) **Facial Recognition Technology's Inaccuracies and Biases** : Currently, facial recognition technology is highly error prone, with both high false positive and false negative rates. It was only a few years ago that state-of-art machine/deep learning algorithms misidentified Queen Elizabeth as a shower cap and labelled people of color as apes. Even when limiting the identification task to faces, Amazon's facial recognition system recently mis-identified over two dozen congressional representatives as criminals[1]. **Machine learning systems largely "learn" on their own, so the decision trees that contribute to errors in final output cannot be traced and corrected.**

Sources of error due to design of facial recognition technology include (a) the datasets that are used to train (teach) the machine learning system; (b) the choice of which features are most critical for a "match"; (c) variations in lighting, resolution, angle and distance. For examples of how these biases affect results, databases and machine learning systems based on mugshots will overrepresent people of color due to the racial bias inherent in the criminal justice system. Further, these databases assume criminality even though the photos are of people who haven't been convicted of any crime. In contrast, databases and machine learning based on driver's license photos will be majority white and therefore will under-specify features associated with people of color, not to mention children. Finally, databases constructed from publicly available photos (e.g., CCTV or Facebook) will exhibit more bias resulting from differences in quality, lighting or other contextual cues. Similarities in hairstyles, clothing, and make-up also can cause mis-matches[2].

In addition, there are also **sources of error due to use,** including (d) automation bias, (e) confirmation bias, and (f) reckless use. Automation bias is the tendency to treat a machine's output as fact, not understanding the potential sources of error outlined above or variations in the types of bias in systems with differences in design. Confirmation bias is the tendency to believe any output provided by the system that supports an already held view or suspicion, regardless of the credibility of the source. Numerous scientists and human rights advocates have indicated facial recognition technology currently lacks credibility.

Given the high error rate of facial recognition technology and the repercussions of a mistake, all use of facial recognition technology is reckless use at this time. On these grounds, fourteen cities including San Francisco and Boston have already banned its use. Forty informed groups have called for a moratorium[3]. Why invest in a technology that isn't reliable, can cause tremendous harm, and which further exacerbates existing societal biases ?

Imagine the semblance you were matched to originated from a mugshot database. And that the people who did the matching were police immediately swarming and surrounding you with tasers and/or guns drawn. Imagine losing your job or the goodwill of your stranger neighbors due to the hullabaloo. Imagine being thrown in jail without the opportunity to inquire or prove they had the wrong person[4]. Police are intuitively going to believe the results of technology that is there to help them, especially when it confirms their already existing biases. Even without facial recognition software, this is already a problem: I clearly remember MPD pulling over and surrounding with guns drawn, a Black woman driving her car home this summer. She had reported her car stolen, and then reported it found before driving it home. Maybe a clerical time delay was at fault or another type of glitch. **The more we rely on databases and software the greater the opportunities for life-altering glitches. The time scale on which police act and the seriousness of potential consequences makes facial recognition an extremely UNWISE choice for Law Enforcement.**

A 2019 NIST (National Institute of Standards and Technology) study evaluating the error rates of different facial recognition systems designed in the U.S. found up to a 100-fold difference in mismatch errors for Black, Asian-American, and Native American adults . False positive rates were also much higher for women, elderly and children[5]. Other studies have found mis-match rates as high as 80% and 95%.

As sympathetic as all of us must be towards cases of missing or trafficked children, the resulting trauma and disruption of mis-identified children and parents is not worth the risk of using facial recognition technology, especially since children are among those showing high false positive rates. "Good intentions are not enough"[6].

B) **Problems created by facial recognition even assuming 100% accuracy** . Some members of the public, including the MPD, may argue against the ban on the basis of a "Nothing To Hide" rationale — a rationale that has been soundly debunked for years[7]. The obvious intrusions of data mining and potential for hacking has only grown in the intervening time. Although facial recognition is only one part of the data puzzle, the use of facial recognition by law enforcement carries the most severe immediate repercussions. Facial surveillance is an unwarranted invasion of privacy with no probable cause. The benefits to police are minor compared to the existential cost to everyone. "The problem with the nothing-to-hide argument is the underlying assumption that privacy is about hiding bad things".

Reasons " *Nothing-To-Hide* " is garbage —
1) Denial of Due Process and Increasing Imbalances in Power: Law enforcement (and the State) already have much more information about any specific individual than individuals have about them without adding facial recognition into the mix. Moreover, police are protected by qualified immunity, a powerful union, and the typically unquestioned authority our society has given the police. Facial recognition technology increases the power imbalance and puts already vulnerable groups at even higher risk.

2) Lack of ownership and understanding of origins: Facial recognition relies on databases the police do not own and the security of those databases will increasingly be vulnerable as data is passed through an increasing number of hands, including creators, data mining, data storage, and data marketing corporations and end users. The problems increase exponentially as a function of hacking, alteration, and deep fakes. Photos can be tagged as "of interest", uprated or down-rated not only by law enforcement, but also by the owners of the databases for a variety of reasons that have little to do with criminal activity[8].

3) Exclusion : "people are prevented from having knowledge about how information about them is being used, and when they are barred from accessing and correcting errors in that data"[9].

4) Distortion of Context : While mugshots and driver's license photos are some of the most used for facial recognition databases, photos from other sources also abound with contextual problems. For example, consider an average person going shopping or to the post office captured on drone footage of a protest. Or on CCTV footage exiting the subway alongside someone on a watchlist. Alternatively, consider the difference in the nature of photos available for an orphan versus a member of a large extended family. Or consider that contextual cues in a photo might imply different things in a law enforcement context versus the actual events at which they were taken. Consider that over-policed BIPOC communities are captured by more surveillance technology than whites and that the wealth of surroundings, or more precisely lack-thereof, is implicitly associated with criminality.

5) Aggregation : "emerges from the fusion of small bits of seemingly innocuous

data" . The entire data landscape is a distortion of data points[10] (and photos) collected by businesses with self-interests other than an accurate representation of an individual, that person's character and life. Data and photos taken out of context create anomalous errors and artifacts that can be impossible for any given individual to track down.

8) Nefarious actors : Once databases exist, there is little to stop their use by stalkers and other nefarious actors, whether in law enforcement or not. People do change, whereas data can be stored forever. As a general rule, **every increase in information technology and every increase in the market forces for the use of a technology increases the 'surface area' of vulnerability (or attack surface) to an extent the human mind isn't readily able to keep up with . What's worse, corporations are increasingly washing their hands of their responsibility for the risks of their creations.** Very recently, multiple hospitals have been frozen out of their patient databases, their doctors and patients essentially held for ransom[11].

10) There is no clear legal or regulatory framework : Data mining is the wild wild West in the middle of a gold or oil rush. We are only beginning to understand its harms. **Our laws and regulatory frameworks are decades behind.**

(11) The existential threat mentioned at the beginning of this letter : As Anna Lauren Hoffmann observes[12], "Privacy is not a horror movie, most privacy problems don't result in dead bodies, and demanding evidence of palpable harms will be difficult in many cases." Without question, however, law enforcement is a context in which the palpable harms of facial recognition could result in a horror movie and dead bodies in real life.

In sum, no matter what law enforcement will try to assure you of a) Police and officials usually have little understanding of the biases and assumptions of the databases and machine/deep learning algorithms used to make identifications; b) Police and officials cannot guarantee the validity and security of the information. As a scientist, it is my firm conclusion that the existence and use of facial recognition technology offers little improvement in solving crime, is at least as likely to create more victims, and dramatically increases the "surface area" of vulnerability (or attack surface) beyond what human minds can cope with.

"As a constitutional principle embodied in the Fourth Amendment's protection from "unreasonable searches and seizures," privacy is meant to do more than create legal walls that mirror physical ones, and is not limited to situations where we are inside our own houses[13]." As the Supreme Court has recognized, the concept of privacy needs to include a "privacy of life" that allows us freedom of association in public spaces and allows us to lose ourselves in the anonymity of a crowd[14].

"Facial recognition is not a benign extension of existing surveillance practices— it's rocket fuel. We should reject anything less than a moratorium."[15] In short, Madison, if wanting to preserve the sanity of society, democracy, free speech, privacy and individual civil rights, should ban facial recognition technology, too.

Sincerely,

Gisela Wilson, PhD
1244 Morrison Ct
Madison, WI 53703

[1] Facial Recognition and Equity (with Matt Cagle) https://digitalcommons.law.scu.edu/htli_alsocialimpact/1/?fbclid=IwAR0qLwMQ2T-fW9emUT5bvJMzS-3cl6PRtBrtD2a9is3YVTeqhgp3tb17AS0

[2] Anna Lauren Hoffmann, "The privacy risks of unchecked facial-recognition technology", https://static1.squarespace.com/static/5b8ab61f697a983fd6b04c38/t/5ca3ddcb15fcc0a59411ff30/1554243020037/HoffmannSeattleTimesFaceRecOpEd.pdf

[3] Angela Chen, "40 groups have called for a US moratorium on facial recognition technology" , https://www.technologyreview.com/2020/01/27/276067/facial-recognition-clearview-ai-epic-privacy-moratorium-surveillance/ ; Letter - https://epic.org/privacy/facerecognition/PCLOB-Letter-FRT-Suspension.pdf

[4] Read the account of Robert Williams, a Black resident of Detroit, as a example of the consequences of a false match; https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/

[5] https://crosscut.com/2020/01/technology-vs-privacy-washington-looks-regulate-facialrecognition-tools-2020; https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-agesex-face-recognition-software ; https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[6] https://crosscut.com/2020/01/technology-vs-privacy-washington-looks-regulate-facialrecognition-tools-2020

[7] Daniel J. Solove, "Why Privacy Matters Even if You Have 'Nothing to Hide'" http://www.woldww.net/classes/Information_Ethics/Solove-ChronicleArticle-NothingToHide.pdf

[8] Kashmir Hill, "The Secretive Company that Might End Privacy as We Know It" https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[9] Daniel J. Solove, "Why Privacy Matters Even if You Have 'Nothing to Hide'" http://www.woldww.net/classes/Information_Ethics/Solove-ChronicleArticle-NothingToHide.pdf

[10] ibid.

[11] Ellen Barry and Nicole Perlroth, "Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack"; https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html

[12] Anna Lauren Hoffmann, "The privacy risks of unchecked facial-recognition technology" https://static1.squarespace.com/static/5b8ab61f697a983fd6b04c38/t/5ca3ddcb15fcc0a59411ff30/1554243020037/HoffmannSeattleTimesFaceRecOpEd.pdf

[13] https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/;*Carpenter v. United States*, 585 U.S. ____ (2018)

[14] ibid.

[15] Anna Lauren Hoffmann, "The privacy risks of unchecked facial-recognition technology" https://static1.squarespace.com/static/5b8ab61f697a983fd6b04c38/t/5ca3ddcb15fcc0a59411ff30/1554243020037/HoffmannSeattleTimesFaceRecOpEd.pdf

From:	Lesaboat@charter.net
Sent:	Tuesday, December 01, 2020 12:48 AM
To:	All Alders
Subject:	[All Alders] Ban of all facial recognition technology use

Recipient: All Alders

Name: Lesa Reisdorf
Address: 1814 Camus Lane, Madison, WI 53705
Phone: 608-232-7449
Email: Lesaboat@charter.net

Would you like us to contact you? No, do not contact me

Message:

I listened to your entire meeting and did a bit of research myself. The technology is not perfect, but if it's used as a tool to help solve crimes and identify victims in conjunction with other evidence that support its results, I think it could be useful with certain limitations. If those guidelines and perimeters are clearly specified in advance with proper training, ongoing observation, data collection and regular review, I think it could be beneficial for our community in protecting children and solving crime. Please do not vote to completely ban it but vote to amend with certain guidelines and designated uses. Thanks.

Veldran, Lisa

From:	Steve Verburg <stverburg@gmail.com>
Sent:	Tuesday, December 01, 2020 1:25 AM
To:	All Alders
Subject:	strictest possible ban on city government use of facial recognition tech

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Good morning,

I'm writing in support of the proposed city of Madison ban on facial recognition technology.

I recently heard Madison Police Department command officers claim without evidence that this technology is an important tool for preventing the exploitation of children. And yet police administrators were unable to give even a rough estimate of the number of such cases they investigate and solve using FR. I'm afraid it strains credulity to hear that a certain sensational crime is widespread in our community, but the police haven't kept track of how many occurrences there have been. The leader of the unit that handles child exploitation purported that she had come to a public meeting to discuss how serious the problem was, but she didn't know how many reported offenses in this category her officers were handling. That seems hard to believe. It's enough to make one suspect that the police hold the public and its elected representatives in low regard. Perhaps they think they can come in and tell Common Council members how scary the world is, and the Common Council will respond by producing another blank check.

It's time to hit the pause button. This is a technology that has significant downsides for civil liberties, freedom and privacy that far outweigh the vague, sensational claims made by Madison police about its supposed benefits.

The strongest possible ban is the best ban.

Consider this statement from the American Civil Liberties Union:
"We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity."

The Georgetown Law Center on Privacy and Technology has also called for a ban as it reported "a dramatic range of abuse and bias has surfaced".

Anna Lauren Hoffmann, a professor at University of Washington Information School, wrote this moving plea: "Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium…. As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me."

This isn't a TV show. This is powerful technology that is bound to be abused, bound to be used against your constituents in the hands of overzealous police, or the next authoritarian state or national leader who rises to power.

Thank-you.

Steve Verburg
1614 Wendy Lane, Madison, Wisconsin
District 16

Veldran, Lisa

From:	Bonnie Roe <bonnie.roe@gmail.com>
Sent:	Tuesday, December 01, 2020 5:21 AM
To:	All Alders; Mayor; Bottari, Mary; Haas, Michael R
Subject:	Please vote NO on ordinance banning Facial Recognition Technology

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders, Mayor, Mayor's Chief of staff, and City Attorney Haas,

Thank you all for the endless hours of work you do on behalf of our City.

Alders, I urge you to please vote no on this sweeping ban of Facial Recognition Technology and take a common sense approach. Or at the very least, table it for further discussion, collaboration, and input from the public and vote at a later date, potentially even the next Common Council meeting. This is too important. As a resident of Madison, I don't want the hands of my police department tied as they work hard to make the community we live in a safer place for all. The exemptions in this ordinance are so limiting to their work. Even in the case of a mass casualty event or exigent circumstances, their hands would be tied from using Facial Recognition Technology to help positively identify a murderer. This is unacceptable to me and seems to even pose liability issues. There would be public outrage. This rushed, overreaching ban will limit law enforcement from using key, cutting-edge technology to fight the most horrible crimes against our residents. It might cause us to have to rely on federal agencies in solving our most heinous crimes, is that what we want?

If we think victims of child human trafficking are worthy of this technology, to aid in finding and rescuing, aren't all of our residents who fall victim to horrible, egregious crime worthy of including this technology as one investigative tool among many? Do we really want to provide cover for those who wish to kill and brutalize our residents?

This technology is new, requiring clear limits, policies, and oversight. But to ban it outright? What if we'd done that with fingerprinting? Or DNA? Where would we be today? In their infancy, these technologies were controversial, now they are common, vital tools. And, like these tools, don't ignore the implications Facial Recognition Technology could have on misidentified perpetrators, who might otherwise be falsely convicted.

Again, here are some great resources that show how it is possible to be progressive in our use of modern and improving technology, while also protecting our privacy rights as citizens. I urge you to take time to consider this issue from all angles.

Presentation by Chief Victor Wahl and Detective Sergeant Julie Johnson at the most recent PSRC meeting, starting at 2:39:47 in the linked video.
https://media.cityofmadison.com/Mediasite/Showcase/madison-city-channel/Presentation/53936094156545ca8b9ede98d5a75e731d

IJIS Institute: Law Enforcement Facial Recognition Use Case Catalog
https://drive.google.com/file/d/1s5LQPykQ9R8OeMcRLOvAeREFb22QJhmh/view?usp=sharing

Security Industry Association: Principles for the Responsible and Effective Use of Facial Recognition Technology
https://drive.google.com/file/d/11OgF-MGZhT3h6jORdsPI3MNJxnWkEvUm/view?usp=sharing

Bureau of Justice Assistance, U.S. Dept. of Justice Policy Development Template:

https://drive.google.com/file/d/1OfTEJVPqmC4UoRCDdGFaP41W8xubhjHG/view?usp=sharing

NYPD Patrol Guide on Facial Recognition Technology:
https://drive.google.com/file/d/1MDrbnoEcleFru-aVTONLwX8L8MmNItJZ/view?usp=sharing

Baltimore Police Department's Letter of Concern regarding banning Facial Recognition Technology:
https://drive.google.com/file/d/1Hub9i2rxzC74Bsm2j-6qXKA5xqXBcBQL/view?usp=sharing

Chicago Police Department's Use of Facial Recognition Technology
https://drive.google.com/file/d/1dwD_nPYpU4Q0iZ-b1aVbngi4mByepkbP/view?usp=sharing

Detroit Police Department Handbook: Policies relating to Facial Recognition Technology
https://drive.google.com/file/d/1A1nVoAtAhJF3lBqCfcMstd200aYiNwSh/view?usp=sharing

Thank you for your consideration,

Bonnie Roe
District 10
608-239-1748

From: Erin Schulten <erin.schulten@gmail.com>
Sent: Tuesday, December 01, 2020 7:28 AM
To: All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject: Banning the use of facial recognition technology

Dear Alders and Mayor,

I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

As Robert Williams, a Black Detroit resident, writes in a Washington Post article:
I was wrongfully arrested because of facial recognition. Why are police allowed to use it?... Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed. What's worse is that, before this happened to me, I actually believed them. I thought, what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?

Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.
The ACLU states:
We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.
Institutions such as the Georgetown Law Center on Privacy and Technology are also calling for a ban, noting that "a dramatic range of abuse and bias has surfaced". As Lindsey Barret of Georgetown Law Center writes in the publication "Ban Facial Recognition Technologies for Children – and Everyone Else":
Clearview AI, which has been heavily criticized for its privacy violative services, has been quick to tout the use of its product in cases involving children, including investigations into child sexual exploitation. The horrendous nature of those crimes may seem to reduce the need for scruples when it comes to the harms of these technologies, when in fact the sensitivity of the circumstances makes their problems even more concerning. The false identification of a victim could be deeply traumatic, and the false identification of an ostensible perpetrator could lead to tremendously damaging consequences for the wrongly identified.
Anna Lauren Hoffmann, a professor at University of Washington Information School, writes:
Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium.... As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.
Facial recognition software produces inaccurate and biased results.
Some people have a mistaken belief that facial recognition technology works as it's portrayed in TV shows like NCIS. Such shows are science fiction – reality is totally different.
Inaccuracy is particularly high with children and the elderly. The 2019 NIST (National Institute of Standards and Technology) report shows that if you use ideal photos (i.e., the best possible conditions) for both a test photo of a child and a database of photos of different children, the typical vendor algorithm will incorrectly call 1% of all photos in the database a match (making this technology close to useless for children). There's also racial bias - existing facial recognition software exhibit greatly elevated error rates with faces of Black folks, and especially Black women.
Moreover, as one article notes of the NIST findings...
accuracy is only possible in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the subjects are clear and unobscured. In real world deployments, accuracy rates tend to be far lower. For example, the FRVT [2019 NIST Facial Recognition Vendor Test] found that the error rate for one leading algorithm climbed from 0.1% [for middle-aged adults] when matching against high-quality mugshots to 9.3% when matching instead to

pictures of individuals captured 'in the wild,' where the subject may not be looking directly at the camera or may be obscured by objects or shadows.

Thus, a 2018 study by a British nonprofit found:

The overwhelming majority of the police's "matches" using automated facial recognition to date have been inaccurate. On average, a staggering 95% of "matches" wrongly identified innocent people... Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people.

Police face recognition will disproportionately harm Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals.

Facial recognition technology constitutes a grave danger to civil liberties

Facial recognition technology infringes on a vital constitutional principle, the right to privacy, raising serious 4th amendment issues. It can permit cataloging of sensitive information and unchecked location tracking. And it can profoundly impact 1st amendment rights - endangering and chilling 1st amendment activities and press freedoms.

In their article “Facial Recognition Is the Perfect Tool for Oppression”, Woodrow Hartzog (Professor of Law and Computer Science at Northeastern University School of Law) and Evan Selinger (Professor of Philosophy at Rochester Institute of Technology) note:

facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented. It's the missing piece in an already dangerous surveillance infrastructure, built because that infrastructure benefits both the government and private sectors. And when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering....

It’s easy to think people don’t have a strong privacy interest in faces because many of us routinely show them in public.... The thing is we actually do have a privacy interest in our faces, and this is because humans have historically developed the values and institutions associated with privacy protections during periods where it’s been difficult to identify most people we don’t know. Thanks to biological constraints, the human memory is limited; without technological augmentation, we can remember only so many faces. And thanks to population size and distribution, we’ll encounter only so many people over the course of our lifetimes. These limitations create obscurity zones.

The Project On Government Oversight (POGO), a nonpartisan watchdog, has issued a report entitled “Facing the Future of Surveillance”. It starkly outlines several of the severe dangers to liberty posed by facial recognition technology. Here's an excerpt:

In last year’s landmark Supreme Court decision Carpenter v. United States, the Supreme Court took on the novel risks surveillance in the digital age pose, fully embracing the right to privacy. In an opinion focused on cellphone tracking, the Court declared that “the [Fourth] Amendment seeks to secure the privacies of life against arbitrary power” (emphasis added), a framing that notably focuses not on certain places or types of conversation, but rather on protecting details of each person’s life against an ever-watching government. Perhaps even more explicitly, the opinion of the Court in Carpenter stated that “a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance.”,,,,

When the Court in Carpenter highlighted that location records “hold for many Americans the privacies of life” (emphasis added), it was emphasizing that Fourth Amendment privacy protections do not focus narrowly on privately owned places, but rather on people themselves, wherever they may be.... In Carpenter, the Court highlighted that “a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner,” and therefore presents heightened risks to privacy. While cell phones may have become an extension of our bodies, our faces require no such metaphor; unlike cellphones, our faces are never able to be turned off, left behind, or cast aside. If our faces can be subjected to the same type of continuous surveillance as cellphones, strong limits on surveillance technology will be necessary to properly rebalance power between the government and the people....

Facial recognition amplifies the concerns of upending privacy and unbalancing power between the government and its citizens in a unique and especially troubling way. The Supreme Court’s key fear in both Jones and Carpenter was that in the course of tracking location, the government would unearth individuals’ most sensitive activities. As Justice Sotomayor highlighted, this form of surveillance could catalog “trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.”... Such data could be used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to applications for background checks, to evaluations for civil service employment opportunities. Equally important is the potentially chilling effect on political and other types of participation, such as religious and community activities....

Facial recognition surveillance threatens to become as powerful a method of finding and tracking individuals as are cellphone and GPS tracking. While the Supreme Court has imposed a warrant requirement for these other forms of electronic location tracking, no such limit exists for facial recognition. In time, facial recognition could become a uniquely powerful location-tracking tool because there is no “middle man” for government-managed cameras that controls access to the data; the entire surveillance system is managed and all relevant information is obtained directly by law enforcement...

A necessary aspect of freedom of expression and association is group anonymity. Over six decades ago, the Supreme Court held that “Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." In that case, NAACP v. Alabama, the key action at issue was the government demanding NAACP's Alabama membership list. In the digital age, no such direct action is necessary to remove the anonymity of an organization's members. A single camera outside the entrance or exit to a group's events combined with facial recognition could produce a membership list without consent or even notification. And because such identification can be done with practically no expenditure of human resources, it can be conducted on a mass scale....

Facial recognition could be a tool to disrupt First Amendment-protected activities. Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and then arrest any individual with an active bench warrant. Ability to effortlessly identify any bench warrant for any petty offense could enable arbitrary action and abusive targeting, such as against selectively targeted individuals attending "events of interest," such as protests, political events, and religious ceremonies. This was already observed on a small scale with Geofeedia—a social media-monitoring company—which admitted that Baltimore police used the service during protests to "run social media photos through facial recognition technology" to find individuals with "outstanding warrants and arrest them directly from the crowd," with the goal of targeting individuals who were protesting. Given the number of bench warrants for petty offenses that some municipalities maintain, it is entirely possible that facial recognition could become an "arrest-at-will" authority used to disrupt such activities on a broad basis....

Modern surveillance powers force journalists to take extra precautions, such as leaving cell phones and other electronic devices with built in GPS at home. But facial recognition can be used not just to catalog activities, but also interactions. If it becomes a tool to pinpoint how individuals interact and meet with journalists, it could present significant roadblocks for journalists seeking to speak to sources and whistleblowers while preserving anonymity.

Face surveillance is a menace disguised as a gift. Its implementation threatens to leave us all less free. Please support a strict ban on the use of this violative technology.

Sincerely,

Erin Schulten
143 Ponwood Circle
Madison, WI 53717

Veldran, Lisa

From: Kara Coffman <karamariahc@gmail.com>
Sent: Tuesday, December 01, 2020 7:40 AM
To: All Alders
Subject: Support for item #76

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Hello, City of Madison Alders--

I would like to express my support for item #76 on tonight's Common Council meeting agenda. Without strong proof that this technology will not be racially biased, facial recognition technology should not be used. Technology always carries the biases of the society that develops it, and we know that facial recognition software is less accurate in identifying black faces. Our criminal justice system is already deeply unfair to people of color. How can we claim to care about inequities in the system and simultaneously deploy a technology that has not been proven to be equitable? I'm not opposed to new technologies, but let's make sure they work well first, that they work for the benefit of everyone.

Thank you,

Kara Coffman

Veldran, Lisa

From:	molly ginsberg <mginsberg888@gmail.com>
Sent:	Tuesday, December 01, 2020 7:51 AM
To:	All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject:	Opposition to Surveillance Technology

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders and Mayor,

I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

As Robert Williams, a Black Detroit resident, writes in a Washington Post article:

I was wrongfully arrested because of facial recognition. Why are police allowed to use it?... Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed. What's worse is that, before this happened to me, I actually believed them. I thought, what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?

Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.

The ACLU states:

We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.

Institutions such as the Georgetown Law Center on Privacy and Technology are also calling for a ban, noting that "a dramatic range of abuse and bias has surfaced". As Lindsey Barret of Georgetown Law Center writes in the publication "Ban Facial Recognition Technologies for Children – and Everyone Else":

Clearview AI, which has been heavily criticized for its privacy violative services, has been quick to tout the use of its product in cases involving children, including investigations into child sexual exploitation. The horrendous nature of those crimes may seem to reduce the need for scruples when it comes to the harms of these technologies, when in fact the sensitivity of the circumstances makes their problems even more concerning. The false identification of a victim could be deeply traumatic, and the false identification of an ostensible perpetrator could lead to tremendously damaging consequences for the wrongly identified.

Anna Lauren Hoffmann, a professor at University of Washington Information School, writes:

Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium.... As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.

Facial recognition software produces inaccurate and biased results.

Some people have a mistaken belief that facial recognition technology works as it's portrayed in TV shows like NCIS. Such shows are science fiction – reality is totally different.

Inaccuracy is particularly high with children and the elderly. The 2019 NIST (National Institute of Standards and Technology) report shows that if you use ideal photos (i.e., the best possible conditions) for both a test photo of a child and a database of photos of different children, the typical vendor algorithm will incorrectly call 1% of all photos in the database a match (making this technology close to useless for children). There's also racial bias - existing facial recognition software exhibit greatly elevated error rates with faces of Black folks, and especially Black women.

Moreover, as one article notes of the NIST findings...

accuracy is only possible in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the subjects are clear and unobscured. In real world deployments, accuracy rates tend to be far lower. For example, the FRVT [2019 NIST Facial Recognition Vendor Test] found that the error rate for one leading algorithm climbed from 0.1% [for middle-aged adults] when matching against high-quality mugshots to 9.3% when matching instead to pictures of individuals captured 'in the wild,' where the subject may not be looking directly at the camera or may be obscured by objects or shadows.

Thus, a 2018 study by a British nonprofit found:

The overwhelming majority of the police's "matches" using automated facial recognition to date have been inaccurate. On average, a staggering 95% of "matches" wrongly identified innocent people... Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people.

Police face recognition will disproportionately harm Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals.

Facial recognition technology constitutes a grave danger to civil liberties

Facial recognition technology infringes on a vital constitutional principle, the right to privacy, raising serious 4th amendment issues. It can permit cataloging of sensitive information and unchecked location tracking. And it can profoundly impact 1st amendment rights - endangering and chilling 1st amendment activities and press freedoms.

In their article "Facial Recognition Is the Perfect Tool for Oppression", Woodrow Hartzog (Professor of Law and Computer Science at Northeastern University School of Law) and Evan Selinger (Professor of Philosophy at Rochester Institute of Technology) note:

facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented. It's the missing piece in an already dangerous surveillance infrastructure, built because that infrastructure benefits both the government and private sectors. And when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering....

It's easy to think people don't have a strong privacy interest in faces because many of us routinely show them in public.... The thing is we actually do have a privacy interest in our faces, and this is because humans have historically developed the values and institutions associated with privacy protections during periods where it's been difficult to identify most people we don't know. Thanks to biological constraints, the human memory is limited; without technological augmentation, we can remember only so many faces. And thanks to population size and distribution, we'll encounter only so many people over the course of our lifetimes. These limitations create obscurity zones.

The Project On Government Oversight (POGO), a nonpartisan watchdog, has issued a report entitled "Facing the Future of Surveillance". It starkly outlines several of the severe dangers to liberty posed by facial recognition technology. Here's an excerpt:

In last year's landmark Supreme Court decision Carpenter v. United States, the Supreme Court took on the novel risks surveillance in the digital age pose, fully embracing the right to privacy. In an opinion focused on cellphone tracking, the Court declared that "the [Fourth] Amendment seeks to secure the privacies of life against arbitrary power" (emphasis added), a framing that notably focuses not on certain places or types of conversation, but rather on protecting details of each person's life against an ever-watching government. Perhaps even more explicitly, the opinion of the Court in Carpenter stated that "a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance.",,,,

When the Court in Carpenter highlighted that location records "hold for many Americans the privacies of life" (emphasis added), it was emphasizing that Fourth Amendment privacy protections do not focus narrowly on privately owned places, but rather on people themselves, wherever they may be.... In Carpenter, the Court highlighted that "a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner," and therefore presents heightened risks to privacy. While cell phones may have become an extension of our bodies, our faces require no such metaphor; unlike cellphones, our faces are never able to be turned off, left behind, or cast aside. If our faces can be subjected to the same type of continuous surveillance as cellphones, strong limits on surveillance technology will be necessary to properly rebalance power between the government and the people....

Facial recognition amplifies the concerns of upending privacy and unbalancing power between the government and its citizens in a unique and especially troubling way. The Supreme Court's key fear in both Jones and Carpenter was that in the course of tracking location, the government would unearth individuals' most sensitive activities. As Justice Sotomayor highlighted, this form of surveillance could catalog "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."... Such data could be used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to applications for background checks, to evaluations for civil service employment opportunities. Equally important is the potentially chilling effect on political and other types of participation, such as religious and community activities....

Facial recognition surveillance threatens to become as powerful a method of finding and tracking individuals as are cellphone and GPS tracking. While the Supreme Court has imposed a warrant requirement for these other forms of electronic location tracking, no such limit exists for facial recognition. In time, facial recognition could become a uniquely powerful location-tracking tool because there is no "middle man" for government-managed cameras that controls access to the data; the entire surveillance system is managed and all relevant information is obtained directly by law enforcement...

A necessary aspect of freedom of expression and association is group anonymity. Over six decades ago, the Supreme Court held that "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." In that case, NAACP v. Alabama, the key action at issue was the government demanding NAACP's Alabama membership list. In the digital age, no such direct action is necessary to remove the anonymity of an organization's members. A single camera outside the entrance or exit to a group's events combined with facial recognition could produce a membership list without consent or even notification. And because such identification can be done with practically no expenditure of human resources, it can be conducted on a mass scale....

Facial recognition could be a tool to disrupt First Amendment-protected activities. Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and then arrest any individual with an active bench warrant. Ability to effortlessly identify any bench warrant for any petty offense could enable arbitrary action and abusive targeting, such as against selectively targeted individuals attending "events of interest," such as protests, political events, and religious ceremonies. This was already observed on a small scale with Geofeedia—a social media-monitoring company—which admitted that Baltimore police used the service during protests to "run social media photos through facial recognition technology" to find individuals with "outstanding warrants and arrest them directly from the crowd," with the goal of targeting individuals who were protesting. Given the number of bench warrants for petty offenses that some municipalities maintain, it is entirely possible that facial recognition could become an "arrest-at-will" authority used to disrupt such activities on a broad basis....

Modern surveillance powers force journalists to take extra precautions, such as leaving cell phones and other electronic devices with built in GPS at home. But facial recognition can be used not just to catalog activities, but also interactions. If it becomes a tool to pinpoint how individuals interact and meet with journalists, it could present significant roadblocks for journalists seeking to speak to sources and whistleblowers while preserving anonymity.

Face surveillance is a menace disguised as a gift. Its implementation threatens to leave us all less free. Please support a strict ban on the use of this violative technology.

Sincerely,

Molly Ginsberg

From:	Lesaboat@charter.net
Sent:	Tuesday, December 01, 2020 8:37 AM
To:	All Alders
Subject:	[All Alders] Ban of all facial recognition technology use

Recipient: All Alders

Name: Lesa Reisdorf
Address: 1814 Camus Lane, Madison, WI 53705
Phone: 608-232-7449
Email: Lesaboat@charter.net

Would you like us to contact you? No, do not contact me

Message:

I listened to your entire meeting and did a bit of research myself. The technology is not perfect, but if it's used as a tool to help solve crimes and identify victims in conjunction with other evidence that support its results, I think it could be useful with certain limitations. If those guidelines and perimeters are clearly specified in advance with proper training, ongoing observation, data collection and regular review, I think it could be beneficial for our community in protecting children and solving crime. Please do not vote to completely ban it but vote to amend with certain guidelines and designated uses. Thanks.

Veldran, Lisa

From:	Lesaboat@charter.net
Sent:	Tuesday, December 01, 2020 8:39 AM
To:	All Alders
Subject:	[All Alders] Ban of all facial recognition technology use

Recipient: All Alders

Name: Lesa Reisdorf
Address: 1814 Camus Lane, Madison, WI 53705
Phone: 608-232-7449
Email: Lesaboat@charter.net

Would you like us to contact you? No, do not contact me

Message:

I listened to your entire meeting and did a bit of research myself. The technology is not perfect, but if it's used as a tool to help solve crimes and identify victims in conjunction with other evidence that support its results, I think it could be useful with certain limitations. If those guidelines and perimeters are clearly specified in advance with proper training, ongoing observation, data collection and regular review, I think it could be beneficial for our community in protecting children and solving crime. Please do not vote to completely ban it but vote to amend with certain guidelines and designated uses. Thanks.

Veldran, Lisa

From:	Jakob Gingrich <jakob.gingrich@gmail.com>
Sent:	Tuesday, December 01, 2020 8:53 AM
To:	All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject:	Please Vote to Ban Facial Recognition Technology

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders and Mayor,
I'm writing to you to urge you to vote **in favor of banning facial recognition technology** at tonight's meeting. Allowing facial recognition technology would cause huge harm to our community, and especially to people of color.

- Facial recognition software produces inaccurate and biased results.
- Facial recognition technology constitutes a grave danger to civil liberties.

Sincerely,

Jakob Gingrich
701 W Main St
Madison, WI

From: Mary Batson <batsonme22@gmail.com>
Sent: Tuesday, December 01, 2020 9:03 AM
To: All Alders
Subject: Ban the use of facial recognition software

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders,

I am writing to support agenda item #76 banning the use of facial recognition software.

Facial recognition tech has a proven record of misidentifying individuals of color and to some extent women as well at a high rate.. It has led to the known wrongful detention and arrest of several individuals and likely far more whose stories have not been publicized.

A faulty tool that adds to the disproportionate and wrongful arrest of people of color has no place in our city.

Sincerely,
Mary Batson

https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

.

Veldran, Lisa

From:	Erin Skarivoda <erin.skarivoda@gmail.com>
Sent:	Tuesday, December 01, 2020 9:49 AM
To:	All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject:	Support Ordinance to Prohibit Face Surveillance Technology!!

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders and Mayor,

I implore that you support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project. Please listen to them.

The ACLU states:

"We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity."

Police face recognition will disproportionately harm Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals.

Facial recognition technology constitutes a grave danger to civil liberties. Facial recognition technology infringes on a vital constitutional principle, the right to privacy, raising serious 4th amendment issues. It can permit cataloging of sensitive information and unchecked location tracking. And it can profoundly impact 1st amendment rights - endangering and chilling 1st amendment activities and press freedoms.

Face surveillance is a tool of white supremacy and general oppression. Its implementation threatens to leave us all less free. Please support a strict ban on the use of this violative technology.

Sincerely,

Erin Skarivoda
Email: erin.skarivoda@gmail.com
Phone: 920-606-1849
Address: 1252 Spaight St, Madison, WI 53703

From:	jhirsch@chorus.net
Sent:	Tuesday, December 01, 2020 10:05 AM
To:	Mayor; All Alders
Subject:	OPPOSE #76 Ban on Use of Face Surveillance Technology

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Mayor and Alders:

Please **OPPOSE Item #76** Establishing a Ban on the Use of Face Surveillance Technology.

There are two ways to evaluate any technology.

1. The technology itself (Facial recognition software)
2. How it is used (Face surveillance).

The word **Surveillance** in the title of the ordinance, rather than **Recognition**, indicates the goal that the authors hope to achieve...*banning the use of the software for surveillance*. In this case, it isn't the software that is objectionable, it's how the software might be used...*for surveillance*.

Look at the exemptions in this proposal. There are SIX. All six exemptions refer to non-surveillance uses....*investigation, authentication, communication, redaction.*

The use of the term "surveillance" brings an array of negative baggage with it. This baggage is then applied to the software, negating any positive uses.

My hope is that the business operations of the City will be open to any new technology which would improve efficiency, increase accuracy and provide cost savings. All technology should be judged by how it is being used and the advantages it brings, not by the negative connotations applied to it. Let's not let the wording of the proposal cloud the advantages that can be achieved by MPD or any City department who might use the software.

Please step back from this proposal and discuss the implications of a wholesale ban. If the goal is to ban surveillance, the proposal should be rewritten.

Thank you.

Janet Hirsch
7311 Cedar Creek Trail

From: Charles James <cjjames@wisc.edu>
Sent: Tuesday, December 01, 2020 10:28 AM
To: All Alders; Martin, Arvina
Cc: Wendy Reichel; Janet Hirsch; Judy Bluel; Bonnie Roe
Subject: Items #76 and #77

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Mayor Rhodes-Conway, dear Alders, December 1, 2020

I understand that there is a proposal before the Common Council (62413) this evening to prohibit the purchase and use of so-called "facial surveillance technology." I urge you to vote ***against*** this proposal.

I have a simple question: what is going on here?

What you call "facial surveillance technology" is usually called "facial recognition technology", and has been in existence for many years. It is just one tool in a huge box of different tools used by public agencies to identify individual members of a community. Other well-known technologies include finger printing, DNA analysis, blood typing, photography, filming, handwriting analysis, etc. What is different about this technology? Why would its use lead to abuse considering the potential ab/use of other earlier technologies, including one of the oldest "software" instruments we have: artist sketches? Having software to analyze a photograph or film clip in order to identify a child or a murder victim or a potential suspect in a criminal investigation is much more reliable than asking an artist to render a drawing based on second-hand witness statements. Why should local authorities not have access to this technology as well? I don't understand the proposed ban. It can't be cost, because many private businesses, even individual community members, can buy it. Again: what is going on here?

As long as I have your attention, I understand that there is also a proposal (62908) to offer a four-year memorandum of understanding between the Madison Police Department and Journey Health Mental Center, Inc. In this case, I urge you to vote ***for*** this proposal.

Whenever there is a mental health crisis in Madison that goes outside the private spaces of individual homes and shows up on public streets, the MPD is routinely, even spontaneously and without reflection, called to intervene. Last year I went on a "ride along" with a local MPD officer which involved just such a case. Family and neighbors could not handle the tense situation we found ourselves entangled in. Although the officer in question was excellent at de-escalating a highly emotional situation, the individual involved needed to be taken into protective custody until they could be transferred to a safe environment like Journey. The relationship between MPD and Journey has worked well over the years. I urge you to support the work between these two agencies.

Respectfully,

Charles J. James

4018 St. Clair

Madison, WI 53711

Veldran, Lisa

From: Evan Flietner <eflietner@gmail.com>
Sent: Tuesday, December 01, 2020 11:37 AM
To: All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject: Support Proposal 76 and Ban Facial Recognition Software!

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders and Mayor,

My name is Evan Flietner. I'm a lifelong resident of Madison's east side. I'm emailing you all to encourage you to **support agenda item 76 at tonight's city council meeting and ban the use of facial recognition surveillance technology by Madison city departments.** Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

As Robert Williams, a Black Detroit resident, writes in a Washington Post article:
I was wrongfully arrested because of facial recognition. Why are police allowed to use it?... Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed. What's worse is that, before this happened to me, I actually believed them. I thought, what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?

Many dozens of civil rights organizations are calling for a ban on the use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.

The ACLU states:
We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.

Institutions such as the Georgetown Law Center on Privacy and Technology are also calling for a ban, noting that "a dramatic range of abuse and bias has surfaced". As Lindsey Barret of Georgetown Law Center writes in the publication "Ban Facial Recognition Technologies for Children – and Everyone Else":
Clearview AI, which has been heavily criticized for its privacy violative services, has been quick to tout the use of its product in cases involving children, including investigations into child sexual exploitation. The horrendous nature of those crimes may seem to reduce the need for scruples when it comes to the harms of these technologies, when in fact the sensitivity of the circumstances makes their problems even more concerning. The false identification of a victim could be deeply traumatic, and the false identification of an ostensible perpetrator could lead to tremendously damaging consequences for the wrongly identified.

Anna Lauren Hoffmann, a professor at University of Washington Information School, writes:
Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium.... As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.
Facial recognition software produces inaccurate and biased results.

Some people have a mistaken belief that facial recognition technology works as it's portrayed in TV shows like NCIS. Such shows are science fiction – reality is totally different.

Inaccuracy is particularly high with children and the elderly. The 2019 NIST (National Institute of Standards and Technology) report shows that if you use ideal photos (i.e., the best possible conditions) for both a test photo of a child and a database of photos of different children, the typical vendor algorithm will incorrectly call 1% of all photos in the database a match (making this technology close to useless for children). There's also racial bias - existing facial recognition software exhibit greatly elevated error rates with faces of Black folks, and especially Black women.

Moreover, as one article notes of the NIST findings...
accuracy is only possible in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the subjects are clear and unobscured. In real-world deployments, accuracy rates tend to be far lower. For example, the FRVT [2019 NIST Facial Recognition Vendor Test] found that the error rate for one leading algorithm climbed from 0.1% [for middle-aged adults] when matching against high-quality mugshots to 9.3% when matching instead to pictures of individuals captured 'in the wild,' where the subject may not be looking directly at the camera or may be obscured by objects or shadows.

Thus, a 2018 study by a British nonprofit found:
The overwhelming majority of the police's "matches" using automated facial recognition to date have been inaccurate. On average, a staggering 95% of "matches" wrongly identified innocent people… Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people.

Police face recognition will disproportionately harm Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals.

Facial recognition technology constitutes a grave danger to civil liberties
Facial recognition technology infringes on a vital constitutional principle, the right to privacy, raising serious 4th amendment issues. It can permit cataloging of sensitive information and unchecked location tracking. And it can profoundly impact 1st amendment rights - endangering and chilling 1st amendment activities and press freedoms.

In their article "Facial Recognition Is the Perfect Tool for Oppression", Woodrow Hartzog (Professor of Law and Computer Science at Northeastern University School of Law) and Evan Selinger (Professor of Philosophy at Rochester Institute of Technology) note:
facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented. It's the missing piece in an already dangerous surveillance infrastructure, built because that infrastructure benefits both the government and private sectors. And when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering….

It's easy to think people don't have a strong privacy interest in faces because many of us routinely show them in public…. The thing is we actually do have a privacy interest in our faces, and this is because humans have historically developed the values and institutions associated with privacy protections during periods where it's been difficult to identify most people we don't know. Thanks to biological constraints, the human memory is limited; without technological augmentation, we can remember only so many faces. And thanks to population size and distribution, we'll encounter only so many people over the course of our lifetimes. These limitations create obscurity zones.

The Project On Government Oversight (POGO), a nonpartisan watchdog, has issued a report entitled "Facing the Future of Surveillance". It starkly outlines several of the severe dangers to liberty posed by facial recognition technology.

Here's an excerpt:
In last year's landmark Supreme Court decision Carpenter v. United States, the Supreme Court took on the novel risks

surveillance in the digital age pose, fully embracing the right to privacy. In an opinion focused on cellphone tracking, the Court declared that "the [Fourth] Amendment seeks to secure the privacies of life against arbitrary power" (emphasis added), a framing that notably focuses not on certain places or types of conversation, but rather on protecting details of each person's life against an ever-watching government. Perhaps even more explicitly, the opinion of the Court in Carpenter stated that "a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance.",,,,

When the Court in Carpenter highlighted that location records "hold for many Americans the privacies of life" (emphasis added), it was emphasizing that Fourth Amendment privacy protections do not focus narrowly on privately owned places, but rather on people themselves, wherever they may be.... In Carpenter, the Court highlighted that "a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner," and therefore presents heightened risks to privacy. While cell phones may have become an extension of our bodies, our faces require no such metaphor; unlike cellphones, our faces are never able to be turned off, left behind, or cast aside. If our faces can be subjected to the same type of continuous surveillance as cellphones, strong limits on surveillance technology will be necessary to properly rebalance power between the government and the people....

Facial recognition amplifies the concerns of upending privacy and unbalancing power between the government and its citizens in a unique and especially troubling way. The Supreme Court's key fear in both Jones and Carpenter was that in the course of tracking location, the government would unearth individuals' most sensitive activities. As Justice Sotomayor highlighted, this form of surveillance could catalog "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."... Such data could be used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to applications for background checks, to evaluations for civil service employment opportunities. Equally important is the potentially chilling effect on political and other types of participation, such as religious and community activities....

Facial recognition surveillance threatens to become as powerful a method of finding and tracking individuals as are cellphone and GPS tracking. While the Supreme Court has imposed a warrant requirement for these other forms of electronic location tracking, no such limit exists for facial recognition. In time, facial recognition could become a uniquely powerful location-tracking tool because there is no "middle man" for government-managed cameras that controls access to the data; the entire surveillance system is managed and all relevant information is obtained directly by law enforcement...

A necessary aspect of freedom of expression and association is group anonymity. Over six decades ago, the Supreme Court held that "Inviolability of privacy in group association may in many circumstances be indispensable to the preservation of freedom of association, particularly where a group espouses dissident beliefs." In that case, NAACP v. Alabama, the key action at issue was the government demanding NAACP's Alabama membership list. In the digital age, no such direct action is necessary to remove the anonymity of an organization's members. A single camera outside the entrance or exit to a group's events combined with facial recognition could produce a membership list without consent or even notification. And because such identification can be done with practically no expenditure of human resources, it can be conducted on a mass scale....

Facial recognition could be a tool to disrupt First Amendment-protected activities. Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and then arrest any individual with an active bench warrant. Ability to effortlessly identify any bench warrant for any petty offense could enable arbitrary action and abusive targeting, such as against selectively targeted individuals attending "events of interest," such as protests, political events, and religious ceremonies. This was already observed on a small scale with Geofeedia—a social media-monitoring company—which admitted that Baltimore police used the service during protests to "run social media photos through facial recognition technology" to find individuals with "outstanding warrants and arrest them directly from the crowd," with the goal of targeting individuals who were protesting. Given the number of bench warrants for petty offenses that some municipalities maintain, it is entirely possible that facial recognition could become an "arrest-at-will" authority used to disrupt such activities on a broad basis....

Modern surveillance powers force journalists to take extra precautions, such as leaving cell phones and other electronic devices with built-in GPS at home. But facial recognition can be used not just to catalog activities, but also interactions. If it becomes a tool to pinpoint how individuals interact and meet with journalists, it could present significant roadblocks for journalists seeking to speak to sources and whistleblowers while preserving anonymity.

Face surveillance is a menace disguised as a gift. Its implementation threatens to leave us all less free. Please support a strict ban on the use of this violative technology.

Sincerely,

Evan Flietner

Veldran, Lisa

From: David Sterken <dgsterken@gmail.com>
Sent: Tuesday, December 01, 2020 11:53 AM
To: All Alders; Mayor
Subject: Support for ordinance 62413, agenda item 76 at today's city council meeting

Caution: This email was sent from an external source. Avoid unknown links and attachments.

I am emailing to voice my support for ordinance 62413 (substitute version), which is agenda item 76 at tonight's city council meeting. I support banning the use of facial recognition software by law enforcement because of this software's well-known biases and other inaccuracies, potential for misuse, and the threats it poses to civil liberties, particularly those of already marginalized groups.

David Sterken

From: Amy Owen <amydowen@hushmail.com>
Sent: Tuesday, December 01, 2020 12:26 PM
To: All Alders
Subject: Supporting item #76 on today's Common Council meeting agenda

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders,
I am writing to ask for your support of item #76 on the agenda for today's council meeting, regarding a ban on facial recognition software by city departments. I have strong concerns about the justice implications of using any tools with such well-documented inaccuracies for Black and Brown faces, especially women. Many years of industry and academic research have established that facial recognition technologies do a poor job of identifying people of color. Please also consider the cost of of these technologies on an already deeply strained budget, and the cost of likely lawsuits against the city if a person is wrongly arrested or incarcerated based on a false match from these technologies. The use of tools that have such widely known flaws is not the right choice for our city, and has a high likelihood of exacerbating our community's already problematic racial disparities in arrests and incarceration.
Thank you,
Amy Owen
3129 Buena Vista St.
Madison, WI 53704

Veldran, Lisa

From:	Sally Herman <sjherman2000@gmail.com>
Sent:	Tuesday, December 01, 2020 12:59 PM
To:	All Alders
Subject:	Ban facial recognition software

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Good afternoon City of Madison Alders,

I am writing today to urge you to vote in favor of banning the use of facial recognition software by the City of Madison, especially including the Madison Police. Facial recognition technology has been proven to be very unreliable, and even more so for people of color. It has the potential to falsely implicate people in crimes, and would do so at higher rates for people of color— a clear case of racial discrimination in a country already rife with racism to which Madison is far from immune.

Please take this necessary step towards justice and vote to ban the use of facial recognition software at tonight's council meeting.

Thank you,

Sally Herman

Veldran, Lisa

From:	ulrike dieterle <ulrike.dieterle@gmail.com>
Sent:	Tuesday, December 01, 2020 12:57 PM
To:	All Alders
Cc:	ulrike dieterle
Subject:	Agenda Item 76 – Common Council Meeting, December 1, 2020

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Agenda Item 76 – Common Council Meeting, December 1, 2020

I urge Council to vote against the proposal to ban the use of face surveillance technology. This is an important tool in any anti-crime toolkit. This proposal is misplaced and untimely, especially now we should be covering half of our faces anyway. I believe facial recognition was instrumental in apprehending some of the people who destroyed State Street businesses, attacked innocent bystanders and toppled Capitol grounds statues. If I were a victim of crime in this city, you bet I would want the MPD to have every tool at their disposal to do their jobs. This technology actually helps to protect my freedom. This proposed ban is unnecessary and misguided. Please vote it down.

Ulrike Dieterle, 323 N Blackhawk Ave, Madison 53705

REPORT OF PUBLIC SAFETY REVIEW COMMITTEE 76. 62413 SUBSTITUTE - Creating Section 23.63 of the Madison General Ordinances establishing a Ban on the Use of Face Surveillance Technology. Sponsors: Max Prestigiacomo, Rebecca Kemble, Tag Evers and Michael E. Verveer November 18, 2020 PSRC Registrants.pdf 62413 Version 1.pdf Attachments: Legislative History 9/29/20 Attorney's Office Referred for Introduction Public Safety Review Committee 10/6/20 COMMON COUNCIL Refer to the PUBLIC SAFETY REVIEW COMMITTEE 10/14/20 PUBLIC SAFETY REVIEW COMMITTEE Refer to the PUBLIC SAFETY REVIEW COMMITTEE 11/18/20 PUBLIC SAFETY REVIEW COMMITTEE RECOMMEND TO COUNCIL TO ADOPT - REPORT OF OFFICER Recommendation: Adopt with recommendation that the language be altered to ensure that current usage of facial recognition technology by the Madison Police can continue. Roll Call Vote: 4:1:3:1 - Ayes - Heck, Mitnick, Anglim, Myadze; Noes - Rickey; Absent: Albouras, Amoah, Harrington-McKinney; Non-Voting - Konke

Veldran, Lisa

From:	Molly Collins <mcollins@aclu-wi.org>
Sent:	Tuesday, December 01, 2020 1:59 PM
To:	All Alders
Cc:	Chris Ott
Subject:	Comments Re: Proposed Section 23.63 of the Madison General Ordinances establishing a Ban on the Use of Face Surveillance Technology
Attachments:	2020_12_1Madison Surv Ban Letter.pdf

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Common Council Members:

I write on behalf of the American Civil Liberties Union of Wisconsin (ACLU) to provide comments regarding the proposed addition of Section 23.63 "Banning the Use of Face Surveillance Technology" to the Madison General Ordinances (the "Ban"). The ACLU works to protect the civil liberties and civil rights of all Wisconsinites and does not support the use of any kind of facial recognition technology for the following reasons.

First, facial recognition technology can be used so pervasively that the technology essentially eliminates any expectation of privacy in public spaces. In many instances, the technology has the practical effect of forcing every person that enters public spaces to walk around with an enlarged copy of their driver's licenses on their shirts and turns the phone in their pocket into a government GPS tracking device. Whatever speculative benefits the technology might have in theory, the technology's dramatic and often imperceptible adverse effects on citizen's civil liberties cannot be overcome.

Second, facial recognition technology is significantly more inaccurate in identifying Black, Indigenous, and people of color, women, young people, older people, and transgender/non-binary persons. These technological shortcomings place these already vulnerable groups in danger of being falsely identified, wrongly arrested, and even jailed by law enforcement officials that use this technology. Even when coupled with safeguards like adding human reviewers to verify the identification of a person recognized by this technology, the technology has remained inaccurate in identifying these groups. In short, facial recognition technology's propensity for false identifications of members of already vulnerable groups is both unacceptable and unavoidable. As such, the Common Council should adopt the Ban.

Third, no matter what database facial recognition technology is run against, the outcomes undermine the civil liberties of the public. If the technology runs against law enforcement mugshot databases, the technology risks magnifying existing racial biases in our criminal justice system. Moreover, if the technology is run against the Department of Motor Vehicle databases, the technology increases the intrusion on the public's right to privacy. In any event, neither option is tenable and as a result, facial recognition technology should not be used by law enforcement officials.

The ACLU thanks the Common Council for this opportunity to comment on the Ban and strongly encourages the Common Council to adopt it.

Respectfully Submitted,

Christopher Ott

Executive Director
American Civil Liberties Union of Wisconsin

--
Molly Collins
Advocacy Director
ACLU of Wisconsin
mcollins@aclu-wi.org
(414) 272.4032 ext. 215
Pronouns: She/Her/Hers

Visit our website at aclu-wi.org
Like our Facebook page or follow us on Twitter

ACLU
Wisconsin

ACLU
Wisconsin

State Headquarters:
207 E. Buffalo Street, Suite 325
Milwaukee, WI 53202-5774
414-272-4032 / Fax 414-272-0182
www.ACLU-WI.org

December 1, 2020

Sent Via Electronic Mail

Attention: Madison Common Council Members
allalders@cityofmadison.com

RE: Written Comments Regarding Proposed Section 23.63 of the Madison General Ordinances establishing a Ban on the Use of Face Surveillance Technology

Dear Common Council Members:

I write on behalf of the American Civil Liberties Union of Wisconsin (ACLU) to provide comments regarding the proposed addition of Section 23.63 "Banning the Use of Face Surveillance Technology" to the Madison General Ordinances (the "Ban"). The ACLU works to protect the civil liberties and civil rights of all Wisconsinites and does not support the use of any kind of facial recognition technology for the following reasons.

First, facial recognition technology can be used so pervasively that the technology essentially eliminates any expectation of privacy in public spaces. In many instances, the technology has the practical effect of forcing every person that enters public spaces to walk around with an enlarged copy of their driver's licenses on their shirts and turns the phone in their pocket into a government GPS tracking device. Whatever speculative benefits the technology might have in theory, the technology's dramatic and often imperceptible adverse effects on citizen's civil liberties cannot be overcome.

Second, facial recognition technology is significantly more inaccurate in identifying Black, Indigenous, and people of color, women, young people, older people, and transgender/non-binary persons. These technological shortcomings place these already vulnerable groups in danger of being falsely identified, wrongly arrested, and even jailed by law enforcement officials that use this technology. Even when coupled with safeguards like adding human reviewers to verify the identification of a person recognized by this technology, the technology has remained inaccurate in identifying these groups. In short, facial recognition technology's propensity for false identifications of members of already vulnerable groups is both unacceptable and unavoidable. As such, the Common Council should adopt the Ban.

Third, no matter what database facial recognition technology is run against, the outcomes undermine the civil liberties of the public. If the technology runs against law enforcement mugshot databases, the technology risks magnifying existing racial biases in our criminal justice system. Moreover, if the technology is run against the Department of Motor Vehicle databases, the technology increases the intrusion on the public's right to privacy. In any event, neither option is tenable and as a result, facial recognition technology should not be used by law enforcement officials.

The ACLU thanks the Common Council for this opportunity to comment on the Ban and strongly encourages the Common Council to adopt it.

Respectfully Submitted,

Christopher Ott
Executive Director
American Civil Liberties Union of Wisconsin

Veldran, Lisa

From: Madeline Sall <maddy@sall.net>
Sent: Tuesday, December 01, 2020 2:17 PM
To: All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject: Ban the Use of Face Surveillance Technology by City Departments

Dear Alders and Mayor,

I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

As Robert Williams, a Black Detroit resident, writes in a Washington Post article:

I was wrongfully arrested because of facial recognition. Why are police allowed to use it?... Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed. What's worse is that, before this happened to me, I actually believed them. I thought, what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?

Many dozens of civil rights organizations are calling for a ban on use of this technology, including the ACLU, American-Arab Anti-Discrimination Committee, American Friends Service Committee, Color of Change, Consumer Federation of America, Council on American-Islamic Relations, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom of the Press Foundation, National Center for Transgender Equality, National LGBTQ Task Force, Restore the Fourth, and Surveillance Technology Oversight Project.

The ACLU states:

We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.

Institutions such as the Georgetown Law Center on Privacy and Technology are also calling for a ban, noting that "a dramatic range of abuse and bias has surfaced". As Lindsey Barret of Georgetown Law Center writes in the publication "Ban Facial Recognition Technologies for Children – and Everyone Else":

Clearview AI, which has been heavily criticized for its privacy violative services, has been quick to tout the use of its product in cases involving children, including investigations into child sexual exploitation. The horrendous nature of those crimes may seem to reduce the need for scruples when it comes to the harms of these technologies, when in fact the sensitivity of the circumstances makes their problems even more concerning. The false identification of a victim could be deeply traumatic, and the false identification of an ostensible perpetrator could lead to tremendously damaging consequences for the wrongly identified.

Facial recognition software produces inaccurate and biased results.

Some people have a mistaken belief that facial recognition technology works as it's portrayed in TV shows like NCIS. Such shows are science fiction – reality is totally different.

Inaccuracy is particularly high with children and the elderly. The 2019 NIST (National Institute of Standards and Technology) report shows that if you use ideal photos (i.e., the best possible conditions) for both a test photo of a child and a database of photos of different children, the typical vendor algorithm will incorrectly call 1% of all photos in the database a match (making this technology close to useless for children). There's also racial bias - existing facial recognition software exhibits greatly elevated error rates with faces of Black folks, and especially Black women.

Police face recognition will disproportionately harm Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals.

Facial recognition technology constitutes a grave danger to civil liberties

Facial recognition technology infringes on a vital constitutional principle, the right to privacy, raising serious 4th amendment issues. It can permit cataloging of sensitive information and unchecked location tracking. And it can profoundly impact 1st amendment rights - endangering and chilling 1st amendment activities and press freedoms.

Face surveillance is a menace disguised as a gift. Its implementation threatens to leave us all less free. Please support a strict ban on the use of this violative technology.

Sincerely,

Madeline Sall, resident of District 6

1253 Williamson St #3 Madison, WI 53703

Madeline Sall
maddy@sall.net

Veldran, Lisa

From: Linda Ketcham <linda@justdane.org>
Sent: Tuesday, December 01, 2020 3:23 PM
To: All Alders; Mayor
Subject: Support of proposed ordinance to prohibit use of facial surveillance technology

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Council Members and Mayor:

I am writing on behalf of JustDane to request your support of the proposed ordinance to prohibit the use of face surveillance technology by City Departments. It is our belief that use of such facial recognition systems pose a real threat to civil liberties and can lend themselves to racial profiling and civil rights violations as have been well documented in other communities. . We ask that you keep the ordinance as written and do not weaken it in any way.

We add our name to the many civil rights organizations that are calling for a ban on the use of facial recognition technology, among them, the ACLU, the American-Arab Anti-Discrimination Committee, Color of Change, Council on American-Islamic Relations, National LGBTQ Task Force, and the American Friends Service Committee.

We are particularly concerned with the high rate of inaccuracy of this technology related to children and the racial bias found in the increased error rates of people of color, particularly among Black women. The majority of police "matches" using this technology to date have been inaccurate resulting in the storage of biometric photos of thousands of innocent people.

I vividly recall sitting in the Mayor's conference room with the previous Mayor, Mayor Soglin, on numerous occasions. As we sat the Mayor would pull up the camera footage/live stream from the surveillance cameras at the top of State Street, sure that the individuals congregated there were engaged in some illegal activity. Most often what I witnessed on that footage/live stream were individuals, most experiencing homelessness, most people of color, sitting and talking with one another. In those meetings Mayor Soglin would demand to know if any of us in attendance knew who those people were. Were facial recognition technology in use at that time I shudder to think how people sitting downtown could have been profiled, not to mention the violation of their right to privacy.

At a time and under an Administration at the Federal level when individuals participating in legal, peaceful protests were both demonized and targeted, use of facial recognition technology would allow more totalitarian leaders to target individuals exercising their 1st Amendment right to free speech. We ask that you support this ordinance as written.

Sincerely,

Linda Ketcham

Executive Director
Madison-area Urban Ministry, Inc. (dba JustDane)
2115 S. Park St.
Madison, WI 53713
608-256-0906
She, her,hers

"Compassion and justice are companions, not choices." Wm. Sloane Coffin

Veldran, Lisa

From:	Amelia Royko Maurer <roykomaurer@mac.com>
Sent:	Tuesday, December 01, 2020 4:18 PM
To:	All Alders
Subject:	Facial Recognition Software
Follow Up Flag:	Follow up
Flag Status:	Flagged

Dear Alders,

Please vote for the ban on facial recognition software authored by Alders Kemble, Prestigiacomo, Evers, Verveer, Foster and Heck and if you must, vote for their substitute.

Please do not vote for Alder Hanek's alternate.

The harm caused by this technology far outweighs any benefits. This technology is especially harmful to BIPOC communities. It's not a matter of opinion, it's a fact.

Every vote against White Supremacy Racism matters. Every. Single. One. This one too. No excuses.

I've copied an exerpt from Dr Greg Gelembiuk's letter. As per usual, he's done his homework.

"**1.** Here is a column by Anna Lauren Hoffmann, an assistant professor in the University of Washington Information School.

https://static1.squarespace.com/.../HoffmannSeattleTimesF...

Excerpt:

The dangers of facial recognition technology cannot be overstated. Prominent critics point to pernicious biases — especially against dark skin or young faces — that haven't been adequately addressed. When tested, Amazon's own "Rekognition" system falsely matched more than two dozen members of the United States Congress with criminal mug shots, including a disproportionate number of members of the Congressional Black Congress. Further work has shown how such systems confuse cultural markers of gender or sexuality (like makeup and hairstyles) with physiological ones, effectively "baking in" harmful stereotypes that limit their effectiveness across populations.

More importantly, facial recognition is not happening in a vacuum. It is plugging into existing surveillance structures that threaten millions of Americans daily, enabling the real-time monitoring of individuals by instantly linking faces up to the many information systems already available. One glance, and your face can be tied quickly to local law enforcement records, FBI files, DMV data, financial information, social media profiles, and more.

None of this is hypothetical. Many state and local police departments already have much of this access — they just need your face to supercharge it.

Worse, these structures are already marked by deep inequality. Surveilling Americans has always been a skewed affair, with certain groups bearing more of the burden than others — from persistent monitoring of religious minorities and communities of color to the invasive questioning heaped upon the poor to the systematic tracking of protesters exercising their rights to speech and assembly. Such inequality cannot be addressed by mere "tweaks" to the system. In fact, if facial recognition worked flawlessly, it would only make matters worse. It would simply "perfect" unfair and stifling patterns of targeting and abuse aimed at historically vulnerable populations.

Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium. Passing watered-down and permissive versions of the bill now will only allow face recognition to penetrate deeper into our lives while unmaking any appetite we might have for regulation in the first place.

As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.

2. 40 groups have called for a US moratorium on facial recognition technology. The groups include the Electronic Freedom Foundation, the Consumer Federation of America, the Freedom of the Press Foundation, Media Alliance, the National LGBTQ Task Force and Patient Privacy Rights.

Article: https://www.technologyreview.com/.../facial-recognition.../

Letter from the 40 groups: https://epic.org/.../face.../PCLOB-Letter-FRT-Suspension.pdf

3. Here is an article by Malkia Devich-Cyril, entitled "Defund Facial Recognition. I'm a second-generation Black activist, and I'm tired of being spied on by the police."

https://www.theatlantic.com/.../defund-facial.../613771/...

4. Article by Birgit Schippers (in the U.K.) "Facial recognition: ten reasons you should be worried about the technology"

https://theconversation.com/facial-recognition-ten...

Excerpt:

The right to privacy matters, even in public spaces. It protects the expression of our identity without uncalled-for intrusion from the state or from private companies. Facial recognition technology's indiscriminate and large-scale recording, storing and analysing of our images undermines this right because it means we can no longer do anything in public without the state knowing about it."

Sincerely,

Amelia Royko Maurer

Veldran, Lisa

From:	Shulamith Ellman <ellman.shulamith@gmail.com>
Sent:	Tuesday, December 01, 2020 4:17 PM
To:	All Alders; Rhodes-Conway, Satya V.; Bottari, Mary
Subject:	Support the Ban on Facial Recognition Technology
Follow Up Flag:	Follow up
Flag Status:	Flagged

Caution: This email was sent from an external source. Avoid unknown links and attachments.

Dear Alders and Mayor,

As an IT worker all too familiar with the dangers of unchecked technological capabilities and a member of the Madison community, I am writing to ask that you support the proposed ordinance to prohibit use of face surveillance technology by City departments. Facial recognition systems constitute a deeply flawed technology that is uniquely dangerous to civil liberties. We need a strict prohibition on its use. Please do not weaken this ordinance.

As Robert Williams, a Black Detroit resident, writes in a Washington Post article:

> **I was wrongfully arrested because of facial recognition.** Why are police allowed to use it?... Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed. What's worse is that, before this happened to me, I actually believed them. I thought, what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?

The ACLU states:

> We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.

Facial recognition software produces inaccurate and biased results. Some people have a mistaken belief that facial recognition technology works as it's portrayed in TV shows like NCIS. Such shows are science fiction – reality is totally different. **Inaccuracy is particularly high with children and the elderly**—negating any purported benefit of stopping child sexual exploitation and risking severe trauma to children inappropriately identified as victims. While the horrific nature of these crimes may incite an emotional response, the sensitivity of the situation demands precision and care that facial recognition can't provide. The 2019 NIST (National Institute of Standards and Technology) report shows that if you use ideal photos (i.e., the best possible conditions) for both a test photo of a child and a database of photos of different children, the typical vendor algorithm will incorrectly call 1% of all photos in the database a match (making this technology close to useless for children). There's also racial bias - existing facial recognition software exhibit **greatly elevated error rates with faces of Black folks, and especially Black women**. Police face recognition will disproportionately harm Black residents, both because of the high and racially biased error rates in this technology and because systems that rely on mug shot databases include a disproportionate number of Black individuals.

A 2018 study by a British nonprofit found:

> **The overwhelming majority of the police's "matches" using automated facial recognition to date have been inaccurate.** On average, a staggering 95% of "matches" wrongly identified innocent people… Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people.

Facial recognition technology infringes on a vital constitutional principle– the right to privacy– raising serious 4th amendment issues. In last year's landmark Supreme Court decision Carpenter v. United States, the Supreme Court upheld Americans' Fourth Amendment rights against the threat of surveillance, and Justice Sotomayor warned that this form of surveillance could catalog "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."

Facial recognition could also be a tool to disrupt First Amendment-protected activities. Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and then arrest any individual with an active bench warrant. Ability to effortlessly identify any bench warrant for any petty offense could enable arbitrary action and abusive targeting, such as against selectively targeted individuals attending "events of interest," such as protests, political events, and religious ceremonies. This was already observed on a small scale with Geofeedia—a social media-monitoring company—which admitted that **Baltimore police used the service during protests to "run social media photos through facial recognition technology"** to find individuals with "outstanding warrants and arrest them directly from the crowd," with the goal of targeting individuals who were protesting.

Facial recognition software is a menace disguised as a gift. All evidence points to the conclusion that this type of surveillance is not effective in promoting public safety. It's only effective in terrorizing the innocent, eroding public trust, and infringing on our Constitutional right to privacy. Please support a strict ban on the use of this violative technology.

Sincerely,

Shulamith Ellman