

# Know Your Rights: Investigate the Use of Facial Recognition in Your Backyard

## A Citizen's Guide

by Freddy Martinez and Ryan Nassar for  
Open the Government

by Beryl Lipton for  
MuckRock News

**OPEN** THE **GOVERNMENT**

**MUCKROCK**

# Executive Summary

Federal, local and state agencies have been quietly acquiring controversial facial recognition technology over the last few years. Little is known about how widespread the use of this controversial technology is. Many police departments share software with other law enforcement bureaus or agencies, sidestepping standard procurement disclosures, while some companies require governments to sign non-disclosure agreements before acquisition. Nonetheless, the public has the right to information about its deployment and implementation. The federal Freedom of Information Act (FOIA) and comparable state laws give people the power to request information from public bodies, such as police departments and the intelligence community.

Open the Government and MuckRock are using FOIA to send public records requests about facial recognition technology to hundreds of police agencies across the country. Hundreds of other agencies, however, remain unaudited. If you would like to know more about the use of facial recognition technology in your community, this guide will provide resources on how to start. It explains how a private citizen can file a request for information, how the request should be structured, the rules governing requests, and possible next steps when an agency responds or does not respond to the request.

The federal Freedom of Information Act—and comparable state laws—give people the power to request information from public bodies.

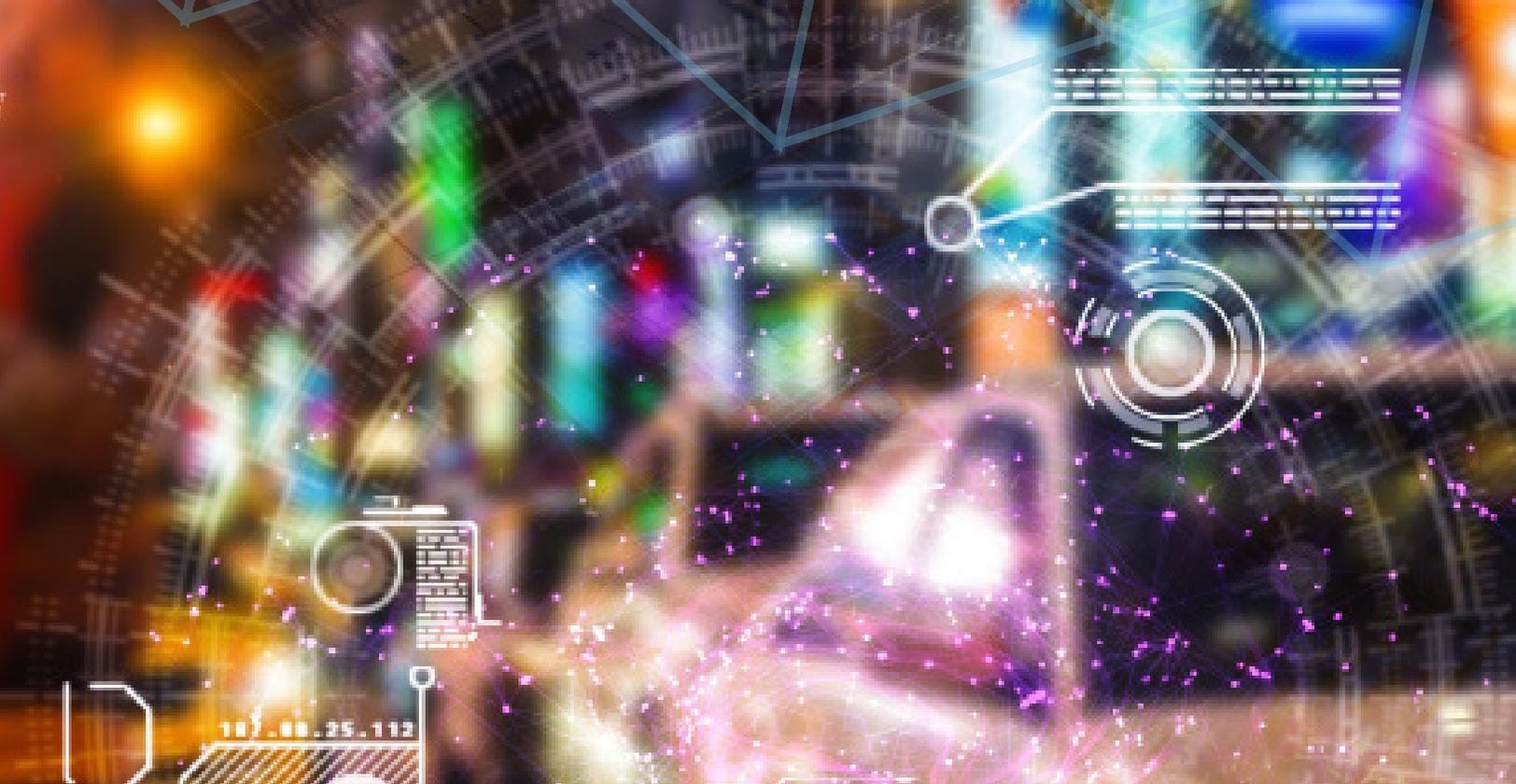
# Facial Recognition Technology

Facial recognition software allows a computing system to analyze a human face by detecting details, such as the distance between the eyes or the shape of the chin, and creating a mathematical representation of its features. Facial recognition technology is used to open iPhones and apply filters to pictures on social media, but it can also be used by law enforcement to identify individuals, both criminal suspects and innocent members of the public.

These algorithms are far from perfect, susceptible to human bias, and can flout expectations of privacy and due process, resulting in serious implications for and violations of the First and Fourth Amendments. There are few laws restricting the use of facial recognition technology, allowing police agencies to implement it however and wherever they see fit. As law enforcement gains new capabilities, it is important to ensure that their acquisition and use are transparent and regulated. Facial recognition has already been used at protests to identify and arrest people, creating a chilling effect on freedom of assembly and speech. Furthermore, if an algorithm were to misidentify a suspect, the justice system could investigate, arrest, and even convict the wrong person, violating individuals' right to be free from unreasonable search and seizures. Currently, there is no consensus from the scientific community on how accurate facial recognition needs to be for it to be admissible in court, potentially depriving defendants of a fair trial.

There is little case law about defendants' right to know they have been identified through facial recognition. Given the serious implications of this technology on our constitutional rights, it is necessary to understand its use across the country.





## Freedom of Information Act

The Freedom of Information Act (FOIA) and its counterparts in all fifty states are valuable tools for gaining information about the activity in which a local, state, or federal body is engaged. They allow public access to documents that a government office might possess but has not released of its own accord. Members of the public can submit a simple information request in order to obtain access to the internal communications, contracts, and financial documents of a government entity - within reason, of course. If you are interested in learning more about your city's police department's use of facial recognition, FOIA is a great place to start. Keep in mind that each state has its own public records law with varying requirements. To learn more, visit MuckRock's [state guides](#).

# Conducting Research

The office charged with responding to your FOIA requests has no obligation to answer questions. They are tasked with providing records in response to record requests so you should be careful to ask for such documents, such as invoices, that would fill in the knowledge gap and help answer your questions. To prepare, familiarize yourself with the applicable public records law.

Along with researching the specific public records laws within your state, it is important to also research the specific documents you are requesting. Public information officers - the people in charge of responding to your FOIA request - do not always personally know the details of the programs in which the public might have an interest. These officers will appreciate requests that try to be specific, and you'll improve your chances of submitting a successful request if you identify or suggest specific records that might exist or the names of entities that may be involved.

For our research, the documents we sought included internal communications about facial recognition technology, solicited and unsolicited marketing material from various facial recognition companies, financial documents detailing purchase orders for the technology, and training manuals for its use. We also requested internal audits for accuracy and bias to better understand if the systems work as advertised.

These records will help us better understand some important elements of facial recognition: the ways it is marketed to government agencies, its associated costs, the instructions for use, and the internal conversation around it. Being as specific as possible will help agencies locate records more quickly and can improve the likelihood you will receive most or all the documents you request.

Records laws usually allow agencies to request some compensation for the work of gathering and sending records, which differs depending on the motivations of the requester. Federal agencies will usually assign you a category — commercial, news media, or “all other” — and you should indicate the category to which you belong in your initial request.

**Companies Selling Facial Recognition Technology**

- DataWorks
- NEC
- Cognitec
- IDEMIA
- Gemalto
- Vigilant Solutions
- Rank One Computing
- FaceFirst
- Amazon (Rekognition)

## FOIA Checklist

- Familiarize yourself with the law.
- Research which documents and companies might be active.
- Draft your request.
- If necessary, follow up with the agency and await a response.
- Review response for completeness.
- If you are willing, share your request and documents with your local news outlet.

## Submitting Your Request

With an understanding of the relevant law and a sense of the records you want, you're ready to submit your request. Almost all agencies will have a contact form or email address to which you can send a request; some may still require submissions by mail or fax. Cite your city or state's FOIA laws, identify the records you would like, and include your fee requester category. Be sure to include that you are seeking the information for non-commercial purposes and that it is in the public interest, which may help you obtain documents with reduced processing fees.

It is good practice to thank the agency for its cooperation and to mention when you expect a response based on the law's legal requirements. That time period will vary between states and the federal government.

While conducting our research surrounding facial recognition technology, we sent 112 requests to police departments across the country. You can find more information about them on the ["Police Surveillance: Facial Recognition Use in Your Backyard"](#) project page on MuckRock.



We have included an example request to help you format your request:

To: [FOIA@chicagopolice.org](mailto:FOIA@chicagopolice.org)

Subject: Freedom of Information Act Request: Facial Recognition Technology

To Whom It May Concern:

Pursuant to the Illinois Freedom of Information Act, I hereby request the following records:

Records and materials related to the solicitation, acquisition, and use of face recognition technology and related software and services. The software or services may be provided by AWS (Rekognition), DataWorks, NEC, and Rank One Computing; this request is applicable to these and any other company providing facial recognition services under consideration or contract with this agency.

Responsive materials include but are not limited to:

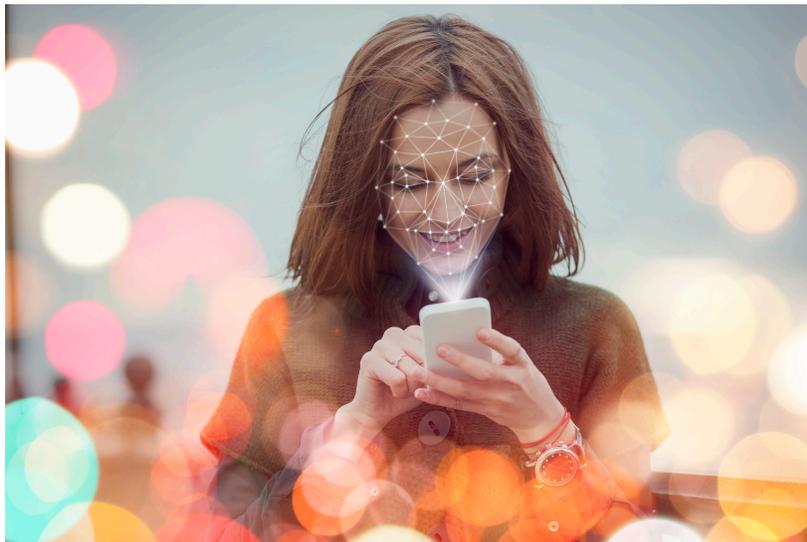
- Agreements: contracts, licensing agreements, nondisclosure agreements.
- Company relations and communications: records related to meetings or follow-up actions with any vendors, companies, or other private entities marketing face recognition to this agency for immigration, intelligence, law enforcement, or other use.
- Financial records: purchase orders, invoices, and other memoranda and documentation.
- Marketing records: All marketing materials - unsolicited, requested, or otherwise - acquired from vendors of face recognition technology.
- Policy records: any policy directives, guidance documents, memoranda, training materials, or similar records governing the use of face recognition technology for immigration, law enforcement, or other purposes. Any memoranda of understanding between this agency and other agencies to share data, access remote systems or other forms of information sharing with external agencies.
- Validation and accuracy: Records, reports, audits, and other documents sufficient to describe validation, accuracy, reliability, and policy compliance of the system.

Please limit the search to records produced from January 1, 2017 – present. Please include in your search as responsive records: communications, memorandums, background papers, meeting minutes, email exchanges, or presentation materials. If your office has questions about this request, please feel free to contact me directly.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 5 business days, as the statute requires.

Sincerely,  
Open the Government



## Response

While FOIA allows private citizens to request data from government agencies, receiving a complete response is not always an easy process. We recommend treating an agency as though it is handling your request in good faith, but you should keep in mind this is not always the case.

Agencies have a statutorily-defined amount of time to respond to your request. Unfortunately, agencies often do not complete requests within this timeframe. The request may be routed to the wrong office. The recipients may not have the resources to complete the request quickly, delay the response, deny the request, reply with no responsive documents or return heavily-redacted documents. It is not uncommon for officers to request multiple time “extensions” for processing your request or fail to provide updates to you.

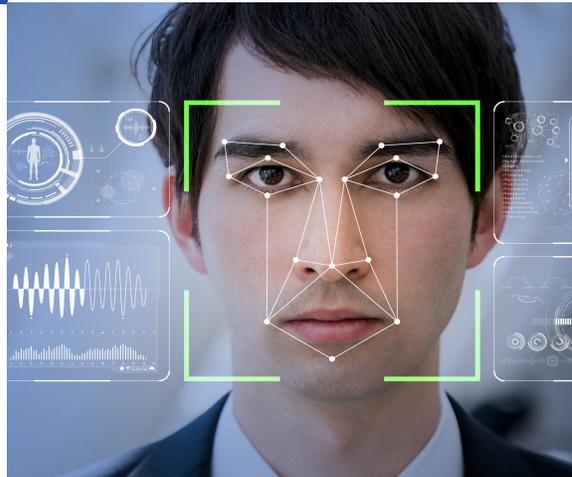
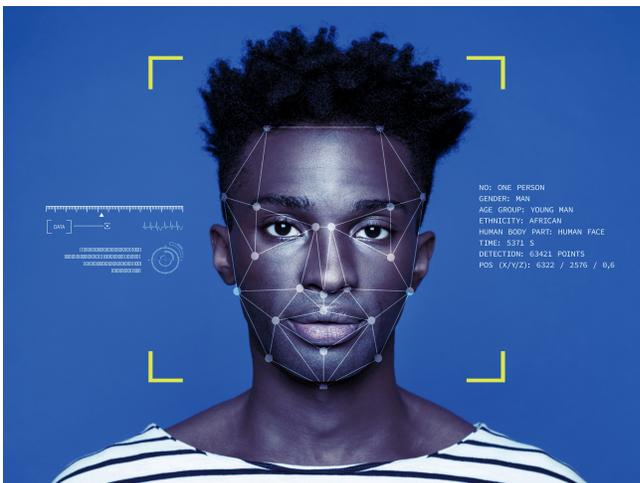
If an agency does not respond to the request, you should be diligent in following up with the agency by phone. If you do not get the documents you requested or the records you receive are incomplete, please contact either [MuckRock News](#) or [Open the Government](#). Both of these organizations have extensive experience in this area and can offer potential next steps (see page 13).

While submitting our FOIA requests to police departments, many responded by saying that they have no records, because they don't have facial recognition technology.

However, just because a police department does not own its own software license, that does not necessarily mean it is not accessing or using the technology. Many police departments do not purchase their own facial recognition systems, and instead will gain access to a larger agency's system, effectively allowing the police department to use facial recognition as it likes. The Columbus Police Department, for example, does not have its own database but uses the data acquired by the Ohio Law Enforcement Gateway (OHLEG), a platform for sharing tools and information between law enforcement agencies. Documents [obtained](#) by MuckRock show dozens of agencies, including the FBI and ICE, have access to OHLEG. While your police department might claim that it does not possess the technology that does not mean it does not have the ability to use it.



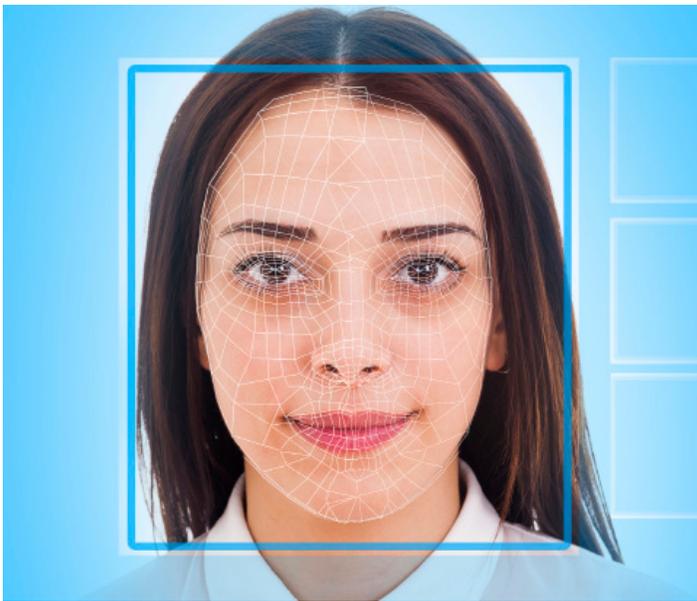
Just because a police department does not own its own software license, that does not necessarily mean it is not accessing or using the technology. Many police departments do not purchase their own facial recognition systems and instead will gain access to a larger agency's system, effectively allowing the police department to use facial recognition as it likes.



## Mixed Results after Sending Over a Hundred Requests

| Status of Requests*         | Number of Requests |
|-----------------------------|--------------------|
| Awaiting Acknowledgement    | 41                 |
| Awaiting Records            | 15                 |
| No Documents Found          | 39                 |
| Records Received            | 10                 |
| Appealed Adequacy of Search | 28                 |
| Fix Required                | 16                 |

\*30 days after sending our requests; some requests appear in more than one category



Requesting information through FOIA is a process that takes time. Not all government or law enforcement agencies will be eager to cooperate with your request. It might be necessary for you to send follow-up emails or call their office to ask about the status of your requests.

You may have to do this several times. If you face significant pushback from agencies, please reach out to our experts who might be able to help you navigate around roadblocks.

The widespread proliferation of facial recognition technology should be of concern to all Americans given its potential to abuse our constitutional rights. Thankfully, access to information is your right, guaranteed to you by the federal and state governments under FOIA. We encourage you to exercise your rights and use this

guide to help hold the government accountable in their continued deployment and use of this invasive technology.

## Contact Us

If you would like more information on any aspect of this guide, or would like to find out more about what you can do, please contact us:

### Open the Government

Email: [info@openthegovernment.org](mailto:info@openthegovernment.org) or call (202) 332-6736  
[www.openthegovernment.org](http://www.openthegovernment.org)

### MuckRock

Email: [info@muckrock.com](mailto:info@muckrock.com)  
[www.muckrock.com](http://www.muckrock.com)