

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Office of Attorney General for the State of New Jersey

Public Input on Regulating Law Enforcement's Use of Facial Recognition Technology

March 11, 2022

The Electronic Privacy Information Center (EPIC) submits these comments in response to the New Jersey Attorney General's request for Public Input on Regulating Law Enforcement's Use of Facial Recognition Technology. EPIC urges the AG's Office to implement a ban on law enforcement use of facial recognition because this technology is 1) fundamentally dangerous and increases disparities in policing, 2) the AG's office will not be able to enforce the proposed regulation, and 3) the proposed regulations will not prevent many of the harms created by facial recognition. A facial recognition ban should apply to all 1:N facial recognition systems used for identification,¹ but need not apply to 1:1 facial comparison systems for identity verification.²

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect

¹ This includes all commercial facial recognition systems like Clearview AI and Vigilant Systems, any state-run facial recognition system, and should also prohibit officers from requesting facial recognition identifications from out-of-state partners.

² For example, an officer using facial recognition to unlock their cellphone, or an agency putting in place a facial recognition system to validate employee entry to sensitive areas would not be prohibited by a ban on facial recognition for identification.

privacy, the First Amendment, and constitutional values. EPIC has long called for bans on the use of facial recognition technology and for clear limitations, transparency, and accountability in its use.³

I. Background

OAG's request for comment regarding facial recognition demonstrates a positive step toward meaningful regulation of the use of biometric technologies as part of law enforcement with New Jersey but remains insufficient in light of the proven dangers that the technology poses.

In 2020, the OAG instructed police departments to halt the use of one particularly egregious widespread facial recognition servicer, Clearview AI.⁴ At least one other town in New Jersey passed a more substantial ban on the use of the company's technology.⁵ These are good and protective steps, but focusing on one problematic servicer ignores the reality of how these services are often accessed, and how common the issues publicized widely in the Clearview scandal are ubiquitous with facial recognition.

³ See, e.g., Ban Face Surveillance, EPIC Campaign, details available at <https://epic.org/banfacesurveillance/>; Testimony of EPIC, Massachusetts Joint Committee on the Judiciary (Oct. 22, 2019), <https://epic.org/testimony/congress/EPIC-FacialRecognitionMoratorium-MA-Oct2019.pdf>; EPIC, *Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology*, Coalition Letter (June 3, 2021), <https://epic.org/privacy/facerecognition/Civil-Rights-Statement-of-Concerns-LE-Use-of-FRT-2021.pdf>; EPIC, *Letter to President Biden on Implementing a Facial Recognition Technology Moratorium*, Coalition Letter (Feb. 16, 2021), <https://epic.org/privacy/facerecognition/Coalition-Letter-Biden-FRT-Moratorium.pdf>, Comments of EPIC to the Office of the Privacy Commissioner of Canada re: Privacy guidance on facial recognition for police agencies (Oct. 15, 2021), <https://epic.org/documents/draft-guidance-to-canadian-police-agencies-on-facial-recognition/>.

⁴ Blake Nelson, *New Jersey cops told to halt all use of controversial facial-recognition technology*, NJ.com (Jan. 25, 2020), <https://www.nj.com/news/2020/01/new-jersey-cops-told-to-halt-all-use-of-controversial-facial-recognition-technology.html>.

⁵ Isiah McCall, *New Jersey cops told to halt all use of controversial facial-recognition technology*, NorthJersey.com (Feb. 25, 2021), <https://www.northjersey.com/story/news/bergen/teaneck/2021/02/25/teaneck-nj-bans-facial-recognition-usage-police-citing-bias/6802839002/>.

Companies like Clearview and countless others provide free trials regularly, and often are used by officers on individual accounts, which could skirt some procurement regulations or even limited or weak prohibitions.⁶

With a specific comment opportunity, OAG is using a transparent process before instituting more permanent regulation of facial recognition technology. While EPIC applauds the transparency here and inclusion of public comment, EPIC will explain below how regulation at the margins around the use is insufficient, and why a ban on the technology is more appropriate.

II. Law enforcement should not use facial recognition technology.

Facial recognition is too powerful for police agencies to use without abuse and harms to privacy and civil liberties. The technology itself is inherently dangerous and should be banned. Further, the public should have a say in approving the technology, and the burden should not be on the public to roll back facial recognition once it is already in place. Facial recognition continues to have serious differential accuracy rates based on race, gender, and age. And even without differential accuracy, facial recognition technology amplifies existing biases in policing.

Facial recognition is inherently dangerous because the technology enables comprehensive public surveillance. With the proliferation of CCTV cameras, pole cameras, cell phones, drones, and surveillance aircraft, public spaces are increasingly surveilled. Facial recognition is the keystone technology that makes mass surveillance useful and cheap. Without it, combing through hours or days of surveillance footage is time consuming and prone to error. In short, facial recognition makes total surveillance a real possibility.

⁶ Ryan Mac, Caroline Haskins, and Antonio Pequeño IV, *Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here.*, BuzzFeed News (Aug. 25, 2021), <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table>.

Ubiquitous identification via facial recognition by the government eliminates the individual's ability to control the disclosure of their identities, creates new opportunities for tracking and monitoring, and increases the security risks from data breaches. An individual's ability to control disclosure of his or her identity is an essential aspect of personal freedom and autonomy. The use of facial recognition erodes these freedoms.

There is little a person in the New Jersey could do to prevent the capture of their image by the government if face surveillance is deployed. Participation in society necessarily requires participation in public spaces. But ubiquitous and near effortless identification eliminates the individual's ability to control the disclosure of their identities to others.

In response, many cities and several states have proactively banned police use of facial recognition.⁷ Major cities including Portland, OR; San Francisco, CA; and Boston, MA have enacted legislation to ban police, or city governments, from using facial recognition technology.⁸ Vermont effectively banned police use of facial recognition in 2020,⁹ and Maine passed a near-total ban in 2021.¹⁰ Bans on law enforcement use of facial recognition are becoming increasingly common as municipalities recognize the harm this technology can cause.

Facial recognition technology amplifies existing biases in policing. Facial recognition systems continue to have differential accuracy rates based on race, gender, and age. Rates of false

⁷ See <https://www.banfacialrecognition.com/map/>.

⁸ See, Shannon Flynn, *13 Cities Where Police Are Banned From Using Facial Recognition Tech*, InnoTech Today (Nov. 18, 2020), <https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/>.

⁹ ACLU of Vermont, *Statement on the Enactment of S.124, The Nation's Strongest Statewide Ban on Law Enforcement Use of Facial Recognition Technology* (Oct. 8, 2020), <https://www.acluvt.org/en/news/aclu-vermont-statement-enactment-s124-nations-strongest-statewide-ban-law-enforcement-use>.

¹⁰ Dave Gershgor, *Maine passes the strongest state facial recognition ban yet*, The Verge (Jun. 30, 2021), <https://www.theverge.com/2021/6/30/22557516/maine-facial-recognition-ban-state-law>.

positives continue to be higher for women, Black and Hispanic people, and the young or old.¹¹ Those errors compound existing biases in policing that negatively impact poor and minority communities. A police force that already disproportionately targets Black folks may be less willing or able to scrutinize facial recognition results wrongfully identifying Black members of the community. When facial recognition results go unquestioned (even through layers of official review), the burden of false identifications, and wrongful arrests, will fall heaviest on people of color.

Beyond accuracy, facial recognition and other advanced surveillance technologies are used disproportionately against poor and minority communities.¹² When license plate readers, pole cameras, and other monitoring tools are deployed more heavily in these communities, they experience more surveillance and overpolicing. Facial recognition can further amplify these effects. If facial recognition is used on mugshot databases, where the poor and minorities are already overrepresented, then the system will create biased results, as poor folks and people of color are more likely to turn up in response to a search. In essence, minority communities will get less privacy, and see disproportionately more arrests and harassment when even very good facial recognition technology is used on biased databases.

¹¹ NIST's 2019 study on demographic effects found that across algorithms, women were 2-5x more likely to be misidentified (a false positive) than men. The same study found that Black people were typically 100x more likely to be misidentified than white people, though results varied somewhat across algorithms. *See NISTIR 8220: Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (2019), <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

¹² In New York, surveillance cameras capable of supporting facial recognition are deployed more heavily in Black and Brown communities, the same communities that are most heavily impacted by stop-and-frisk and other forms of overpolicing. Amnesty International, *Inside the NYPD's Surveillance Machine* (Feb. 14, 2022), <https://banthescan.amnesty.org/decode/>. In Oakland, automated license plate readers are used far more heavily in Black and Brown communities than in wealthier, whiter communities. Dave Maass and Jeremy Gillula, *What You Can Learn from Oakland's Raw ALPR Data*, Electronic Frontier Foundation (Jan. 21, 2015), <https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data>.

III. The Attorney General's Office will not be able to meaningfully enforce the proposed regulations.

It will be difficult for the Attorney General's Office to oversee compliance with the proposed regulations. A ban on facial recognition would be far easier to enforce. Police agencies using facial recognition have long avoided oversight and neglected compliance with the law. Agencies and individual officers have strong incentives to clandestinely abuse facial recognition technology. It is unsurprising that they have regularly adopted facial recognition technology without consultation from civil society or regulators, actively worked to keep their use of the systems secret, broken privacy laws, and failed to oversee individual officers' use of the systems. Given these compliance failures, a ban on facial recognition technology is the only reasonably enforceable option.

The incentives facing police agencies and officers weigh in favor of opacity and non-compliance with the law. Facial recognition, though flawed, is still remarkably powerful: systems like Clearview AI can deliver identities alongside entire social media histories from a single search. With this power comes temptation for police officers who face pressure to identify suspects and solve cases quickly. These intense, short-term incentives to abuse facial recognition technology are balanced against speculative and abstract threats of punishment that will only come if the public learns of the abuses.

These incentives have led to the expected results: police agencies have demonstrated their resistance to regulation by adopting facial recognition systems secretly. By failing to subject themselves to public scrutiny before adopting novel, highly invasive surveillance technologies, police have demonstrated that they cannot be trusted with those technologies. In the United States, more than 1,800 federal, state, and local agencies have used facial recognition technologies without

meaningful oversight or public notice.¹³ The Royal Canadian Mounted Police violated Canada’s Privacy Act by using Clearview AI and lying about it.¹⁴ And dozens of European agencies began using facial recognition unannounced in likely violation of the General Data Protection Regulation (“GDPR”).¹⁵ In Detroit, police misidentified and arrested an innocent man for theft based on facial recognition technology, despite consistent warnings that similar systems are inaccurate when used on Black faces.¹⁶ This is an unfortunately common occurrence, but not a surprising one given the incentives that push police to use these technologies in improper ways. Across jurisdictions and products, law enforcement agencies have shown a consistent policy of secrecy and non-compliance with law when it comes to facial recognition technology.

Even when higher-ups at police agencies adopt facial recognition policies, they are often unable to stop individual employees from abusing the technologies. One problem is the structure of the facial recognition marketplace: companies such as Clearview AI regularly offer free trial accounts directly to individual officers.¹⁷ For example, an instructor with the Washington National Guard Counterdrug Program managed to secretly obtain a free trial of Clearview AI and included information about how to do so in materials for an officer training course.¹⁸ These accounts are

¹³ Ryan Mac, Caroline Haskins, Brianna Sacks & Logan McDonald, *How A Facial Recognition Tool Found Its Way Into Hundreds Of US Police Departments, Schools, And Taxpayer-Funded Organizations*, BuzzFeed News (Apr. 9, 2021), <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition>.

¹⁴ Daniel Therrien, *Special Report to Parliament on the OPC’s Investigation Into the RCMP’s Use of Clearview AI and Draft Joint Guidance for Law Enforcement Agencies Considering the Use of Facial Recognition Technology*, Office of the Privacy Commissioner of Canada (June 10, 2021), https://priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.

¹⁵ Ryan Mac, Caroline Haskins, and Antonio Pequeno IV, *Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here*, BuzzFeed News (Aug. 25, 2021), <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table>.

¹⁶ Adi Robertson, *Detroit Man Sues Police for Wrongfully Arresting Him Based on Facial Recognition*, Verge (Apr. 13, 2021), <https://www.theverge.com/2021/4/13/22382398/robert-williams-detroit-police-department-actu-lawsuit-facial-recognition-wrongful-arrest>.

¹⁷ Mac, Haskins, Sacks & McDonald, *supra* note 13.

¹⁸ *Id.*

virtually impossible for agencies to detect or prevent. A survey from the Government Accountability Office found that even well-resourced federal agencies were unable to track employees' use of facial recognition technologies.¹⁹ In a BuzzFeed News investigation, 34 agencies said that were unaware that their agents had signed up for facial recognition trials until journalists' questions prompted them to look.²⁰ Law enforcement trainings on facial recognition already flatly recommend constitutional violations. For example, in a podcast from the influential Street Cop Training organization, billed as "The training that cops deserve," a trainer recommended officers use facial recognition during traffic stops without reasonable suspicion.²¹ The organization, which advocates a "warrior mentality," suggests facial recognition companies to use in its training handbook.²² Dennis Benigno, a former New Jersey officer, is the organization's founder and lead instructor.²³

The proposed regulations can easily be met without changing abusive surveillance practices. A prohibition on arrests based solely on facial recognition matches, for example, can be flouted with parallel construction—a distressingly common tactic used throughout the policing world.²⁴ Parallel construction could also evade the requirement to produce relevant search queries in discovery. And even after certain officers have been trained in face comparison and identification, they will still be subject to the pressures to evade the law.

¹⁹ Government Accountability Office, *Facial Recognition Technology* 20–21 (2021), <https://www.gao.gov/assets/gao-21-518.pdf> at 20.

²⁰ Ryan Mac, Caroline Haskins, Briana Sacks & Logan McDonald, *Your Local Police Department Might Have Used This Facial Recognition Tool To Surveil You. Find Out Here*, BuzzFeed News (Apr. 6, 2021), <https://www.buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table>.

²¹ Caroline Haskins, *A Popular Workshop for Police Encouraged Cops to Use Face Scans to ID People They Pull Over at Traffic Stops*, Insider (Feb. 2, 2022), <https://www.businessinsider.com/police-workshop-street-cop-training-podcast-facial-recognition-traffic-stops-2022-2>.

²² *Id.*

²³ Street Cop Training, *Instructors* (2019), <https://streetcoptraining.com/instructors/>.

²⁴ Human Rights Watch, *Dark Side: Secret Origins of Evidence in US Criminal Cases* (Jan. 9, 2018), <https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases>.

The New Jersey Attorney General’s Office does not have the resources to implement detailed, independent auditing practices. As already discussed, ensuring that agencies and individual officers may require close monitoring. Right now, that would mean monitoring compliance with each proposed regulation for tens of thousands of officers in about 577 separate police agencies across the state.²⁵ Without a massive increase in the Attorney General’s Office budget, such an oversight regime is not likely to be successful.

IV. Even if enforced, the proposed regulations will not prevent many of the harms caused by police use of facial recognition.

Many of the proposed protections will only apply at the trial stage, but facial recognition can cause many injuries other than wrongful conviction. EPIC supports transparency and disclosure of the technology used during a criminal investigation, but the requirement to record searches and disclose them during discovery are not a meaningful protection against the harms of misidentification. As wrongful arrests from facial recognition in New Jersey and across the country demonstrate, a case need not go to trial to result in serious injuries. A 2019 misidentification of Paterson, NJ resident Najeer Parks led to a wrongful arrest, 10 days in jail, and according to his lawsuit against the city, even subjected him to intense harassment leading Mr. Parks to fear he would be tortured while he was being questioned.²⁶ Time in jail, police harassment, and the risk of police violence are severe harms that cannot be mitigated by even the most rigorous transparency and disclosure requirements.

²⁵ Federal Bureau of Investigation, *Crime Data Explorer*, <https://crime-data-explorer.fr.cloud.gov/pages/explorer/crime/crime-trend> (searching “New Jersey”).

²⁶ Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. Times (Dec. 29, 2020), <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>; Carly Baldwin, *Man Sues Woodbridge Police After Facial Recognition Arrest*, Patch (Jan. 19, 2021), <https://patch.com/new-jersey/woodbridge/man-sues-woodbridge-police-after-facial-recognition-arrest>.

Najeer Parks is among a number of Black men across the national wrongfully arrested based on facial recognition misidentifications. Robert Williams of Detroit was detained for more than 30 hours based on a false match from a low-quality target photo.²⁷ Another Detroit resident, Michael Oliver, eventually lost his job and couldn't make payments on his car after being misidentified and wrongfully arrested based on a facial recognition search.²⁸ The facial recognition search was disclosed during his prosecution, but even clear physical differences between Mr. Oliver and images of the suspect—like full sleeve tattoos—did not prevent police and prosecutors from pushing ahead with his case.²⁹ Simply being identified and pulled into the criminal justice system is a serious harm with life-altering consequences, and a harm that the proposed regulations will not adequately prevent.

Vendor accuracy requirements do not prevent the use of low-quality target images, leaving substantial room for error and bias. EPIC applauds the AG's Office for carefully considering the value of vendor accuracy testing for facial recognition, and producing an accessible summary of NIST's accuracy testing and potential thresholds.³⁰ The latest NIST reports use a variety of datasets to assess the accuracy of facial recognition algorithms, including both high quality images like passport photos, and lower quality images drawn from immigration lane cameras.³¹ While the best algorithms performed very well on controlled mugshot images, the same algorithms had error rates above 20 percent “for side-view images, poorer quality webcam images, and, particularly, for newly

²⁷ Adi Robertson, *Detroit man sues police for wrongfully arresting him based on facial recognition*, The Verge (Apr. 13, 2021), <https://www.theverge.com/2021/4/13/22382398/robert-williams-detroit-police-department-acclu-lawsuit-facial-recognition-wrongful-arrest>.

²⁸ Natalie O'Neill, *Faulty Facial Recognition Led to His Arrest—Now He's Suing*, Vice (Sept. 4, 2020), <https://www.vice.com/en/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing>.

²⁹ *Id.*

³⁰ See New Jersey Office of Attorney General, Public Input on Regulating Law Enforcement's Use of Facial Recognition Technology, *Additional Questions*.

³¹ NIST, Face Recognition Vendor Test (FRVT) Part 2: Identification, NISTIR 8271 DRAFT SUPPLEMENT at 5 (Feb. 2022) https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

introduced ATM-style kiosk photos that were not originally intended for automated face recognition.”³² NIST’s testing reveals that even the best algorithms are only as good as the reference image. While setting high thresholds for accuracy may prevent some misidentifications, low-quality target images continue to pose a substantial threat of wrongful identification, arrest, and in the worst cases, wrongful conviction.

And image quality is not a feature that the AG’s Office can effectively monitor or regulate. With thousands of law enforcement officers spread across 21 counties and 541 municipalities in New Jersey, the AG’s Office lacks the resources to ensure that officers decline to use low-quality images. Such images will make up a substantial portion of law enforcement interest, as CCTV cameras, side-view profiles from cell phones, and other imperfectly captured images from pole or traffic cameras are commonly collected by police. The most up-to-date facial recognition testing makes clear that the risk of error remains unacceptably high.

The proposed prohibitions on “dragnet” and “real time” surveillance still leave room for significant abuses of facial recognition systems. EPIC agrees that bulk surveillance and real time surveillance have substantial negative impacts on privacy and civil liberties but urges the AG’s Office to consider the multitude of other harms caused by facial recognition. Targeted investigations often violate privacy and civil liberties. Across the country, facial recognition has been regularly used to surveil protesters and activists in specific, but pretextual, criminal investigations.

In August 2020, the NYPD used facial recognition to identify racial justice activist Derrick Ingram, who police accused of assault on an officer for using a bullhorn in the officer’s proximity during a protest.³³ That identification led to a “siege” on the activist’s apartment involving dozens of

³² *Id.*

³³ George Joseph and Jake Offenhartz, *NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist’s Apartment*, Gothamist (Aug. 14, 2020), <https://gothamist.com/news/nypd-used-facial->

police officers, helicopters, and an hours-long standoff.³⁴ Mr. Ingram’s identification was accurate, and part of an official investigation, but likely would not have occurred without the use of facial recognition technology.

In June 2020, a secret facial recognition system was used to identify a protester in the infamous Lafayette Square protest in Washington, D.C.³⁵ Many other examples are known, and due to the often opaque nature of facial recognition searches, many more uses of the technology to identify protesters and chill speech will never be known.³⁶ Facial recognition is a go-to tool for policing protests because it can identify a face out of a crowd when few other methods of identification are possible. The proposed regulations might stop bulk or real-time protest surveillance, if they can be enforced, but they will not prevent police from using the technology on protesters in highly pretextual investigations.

In sum, the proposed format for facial recognition regulations is insufficient to protect individuals from harms including wrongful arrest, intensive public surveillance, over-policing, and misuse of the technology. The Attorney General’s Office can take a strong step to protect the public by implementing a full ban on law enforcement use of facial recognition.

[recognition-unit-in-siege-of-black-lives-matter-activists-apartment](#); and Liam Stack, Annie Correal, and Juliana Kim, *N.Y.P.D. Besieges a Protest Leader as He Broadcasts Live*, <https://www.nytimes.com/2020/08/07/nyregion/nypd-derrick-ingram-protester.html>.

³⁴ *Id.*

³⁵ Justin Jouvenal and Spencer Hsu, *Facial recognition used to identify Lafayette Square protester accused of assault* (Nov. 2, 2020), https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html#comments-wrapper.

³⁶ See e.g., Sidney Fussell, *Did a University Use Facial Recognition to ID Student Protesters?*, *Wired* (Nov. 18, 2020), <https://www.wired.com/story/did-university-use-facial-recognition-id-student-protesters/>; Jana Winter, *Facial recognition, fake identities and digital surveillance tools: Inside the post office’s covert internet operations program*, *Yahoo News* (May 18, 2021), <https://news.yahoo.com/facial-recognition-fake-identities-and-digital-surveillance-tools-inside-the-post-offices-covert-internet-operations-program-214234762.html?guccounter=1>; Mike Holden, *Pittsburgh police used facial recognition technology during Black Lives Matter protests*, *WXPI News* (May 21, 2021), <https://www.wpxi.com/news/top-stories/pittsburgh-police-used-facial-recognition-technology-during-black-lives-matter-protests/VT52MGWM3VCDJINJSZPOO5NHKU/> (revealing that Pittsburgh Police used Clearview AI to identify protesters in violation of a city ban on Clearview).

Conclusion

EPIC urges the New Jersey Attorney General's Office to expand on the substantial step of banning Clearview AI by banning all use of facial recognition for identification by law enforcement. Experts, activists, advocates, and impacted communities all agree that a ban is the only action that can prevent the multitude of harms to privacy, civil liberties, and safety caused by law enforcement use of facial recognition. EPIC urges the AG's Office to consider that enforcing detailed regulations on the use of facial recognition would be all but impossible and would still permit harms that will fall heaviest on poor and minority communities.

Respectfully Submitted,

Ben Winters

Ben Winters
EPIC Counsel

Jake Wiener

Jake Wiener
EPIC Law Fellow

Thomas McBrien

Thomas McBrien
EPIC Law Fellow