DHS OPEN FOR BUSINESS

How Tech Corporations Bring the War on Terror to Our Neighborhoods

ACRE ACTION CENTER ON RACE & THE ECONOMY

LittleSis

Media Justice

THE SURVEILLANCE, TECH, & IMMIGRATION POLICING PROJECT AT THE IMMIGRANT DEFENSE PROJECT IDP

This report was co-written by the **Action Center on Race & the Economy (ACRE), LittleSis, MediaJustice,** and the **Surveillance, Tech, and Immigration Policing Project at the Immigrant Defense Project.**

Report Authors

Alli Finn
Surveillance, Tech, and Immigration Policing Project at IDP

Munira Lokhandwala
LittleSis

Aly Panjwani
ACRE

Rumsha Sajid
MediaJustice

Contributors

Mizue Aizeki
Surveillance, Technology, and Immigration Policing Project at IDP

Tracey Corder
ACRE

Myaisha Hayes
MediaJustice

Ramah Kudaimi
ACRE

Jessica Quiason
ACRE

We would like to thank Muslim Justice League, the Stop LAPD Spying Coalition, American Friends Service Committee, Detroit Community Technology Project, Just Futures Law, Muslims for Just Futures, Muslim Counterpublics Lab, the Imagining Freedom, Radical Thought Collective, McKenzie Funk, and Jack Poulson for their thoughtful and valuable feedback on this project.

ACRE is a campaign hub for organizations working at the intersection of racial justice and Wall Street accountability. We provide research and communications infrastructure and strategic support for organizations working on campaigns to win structural change by directly taking on the financial elite that are responsible for pillaging communities of color, devastating working class communities, and harming our environment. www.acrecampaigns.org

LittleSis, also known as Public Accountability Initiative, is a nonprofit public interest research organization focused on corporate and government accountability. PAI maintains LittleSis.org, a free database detailing the connections between powerful people and organizations. Visit us at www.public-accountability.org and www.littlesis.org.

MediaJustice boldly advances racial, economic, and gender justice in a digital age by fighting for just and participatory platforms for expression. We harness community power through the MediaJustice Network of more than 70 local organizations to claim our right to media and technology that keeps us all connected, represented and free. www.mediajustice.org

The Surveillance, Tech, and Immigration Policing Project (STIP) is housed at the **Immigrant Defense Project**, a nonprofit based in New York City. STIP challenges the growing surveillance state by focusing on policing and migrant control, and tackles the rapidly expanding role of technology corporations in undermining local governance. The project supports organizing to build collective public knowledge and political infrastructure to end state violence and to grow a just digital future. See more info here: https://www.immigrantdefenseproject.org/surveillance-tech-immigration-policing/.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In the aftermath of 9/11, the George W. Bush administration launched the global "War on Terror,"[1] capitalizing on public fears and calls for retaliation to justify military intervention and Islamophobic violence across the world. This war demonized and targeted Muslims, both abroad and in the United States. In 2002, the administration founded the Department of Homeland Security (DHS), forcibly reframing federal immigration services, emergency response, and data analysis under a mission to "secure the homeland."[2] This reorganization codified the false link between immigration and terrorism. Instead of making people safe, DHS and its corporate partners used "counterterrorism"[3] to expand policing and surveillance in neighborhoods across the country, targeting immigrant and Muslim communities and intensifying the War on Terror at our doorsteps.

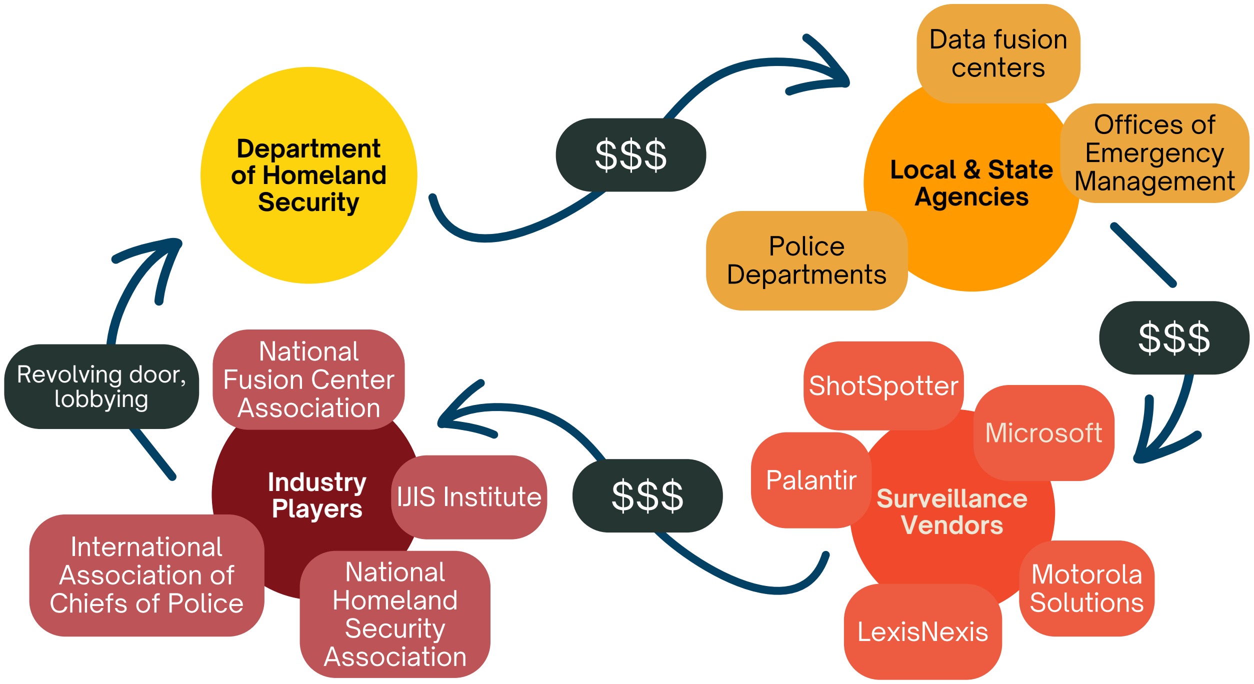
Since its founding, DHS has relied on a state of "emergency" to carry out its operations. Twenty years later, this state of "emergency" has not ended and **immigration policing, "national security," and surveillance have become big business**.

Our report investigates how DHS funding and corporations drive demand for "homeland security," expanding militarized policing in our communities.[4] Through our research, we found that DHS fueled a massive influx of money into surveillance and policing in our cities, under a banner of emergency response and counterterrorism—and with the support of its corporate partners like **Microsoft, LexisNexis, ShotSpotter, Palantir, and Motorola Solutions.**

Specifically, this report presents data on how DHS funneled billions in grant funding to our cities through programs like the **Urban Area Security Initiative (UASI)**. We found that DHS and local policing agencies use this "counterterrorism" grant program to expand surveillance, supercharge militarized police departments, and funnel money right back to the same corporations that advocate for this funding. We focus our research findings on four cities—Los Angeles, Boston, New York City, and Chicago—documenting how **UASI grants intensify local policing and benefit corporations.** We spotlight data fusion centers—institutions that enable interagency information sharing and are **heavily funded by UASI**—as an example of how industry and government collaborate to build systems that criminalize Muslim, Black, Brown, Indigenous, and immigrant communities in our neighborhoods..

The DHS annual budget ballooned from $19.5 billion in 2002 to almost $100 billion in 2023, **channeling much of these funds into corporate pockets**.[5] Our research investigates the role of corporations in creating demand for "homeland security" technology and DHS, from even before 9/11 to today. Our research found that corporations including **Microsoft**, **LexisNexis**, and **Motorola Solutions**, which market themselves as working for the public good, collectively **make billions in revenue** through DHS and government contracts for policing and surveillance—including through contracts and programs funded by UASI. We tell the story of how tech corporations fund and collaborate with law enforcement associations and think tanks, **aggressively supporting the expansion of the "homeland security" machine through DHS grant funding and data fusion centers**. Flush with public funds funneled through DHS, corporations help create the booming industry of policing and mass surveillance in our communities.

In the last twenty years, DHS has devastated our communities through surveillance, police militarization, and deportation; these harms make clear to us that "homeland security" doesn't make us safer, but it does make corporations richer. This report provides organizers and policymakers an understanding of the role that corporations play in shaping "homeland security" policy, adding evidence to growing calls for action to **shut off "counterterrorism" funding pipelines that result in more contracts for corporations and bring militarized policing into our neighborhoods.**



KEY FINDINGS

1. Tech corporations like Microsoft, LexisNexis, and Motorola Solutions drove DHS demand for "homeland security" technologies in the aftermath of 9/11, setting up a revenue stream for their products that continues to today.

Building on decades of research on the role of corporations in the War on Terror, our analysis found that in the wake of 9/11 tech corporations like **Microsoft**—who had recently seen their revenues plummet when the dot-com bubble burst in the early 2000s—positioned themselves as key partners to the government, capturing new revenue streams. Corporations helped develop "homeland security" infrastructure, like data sharing systems, and secured the first contracts with DHS for software technology.[6] Companies like **LexisNexis** pushed the federal government for counterterrorism technologies, through lobbying and research advertising their products, and built new arms of their business to meet the demand they were helping construct. **Motorola Solutions** lobbied for increased DHS funding for its "communications interoperability" technology. **Through relentless lobbying and a revolving door, these same corporations then received millions in contracts from DHS in subsequent decades.**

2. DHS "counterterrorism" grant funding inflates the bloated budgets of local law enforcement agencies, expanding the police and deportation state in our neighborhoods in the name of "emergency" response. Specifically, the Urban Area Security Initiative (UASI), a DHS grant funding program, helps increase profits of surveillance corporations that, in turn, advocate for its continuation.

Through an analysis of UASI funding in Los Angeles, Boston, New York City, and Chicago, we found that cities spend millions of UASI dollars on contracts with surveillance corporations like **ShotSpotter**, **Motorola Solutions**, and **Palantir**. UASI is a part of DHS's **Homeland Security Grant Program (HSGP)**, which has provided almost **$28 billion in funding to local and state agencies since the department's founding.**[7] UASI provides **$615 million** annually to local and state agencies for "counterterrorism" activities, which funds massive purchases of surveillance technology and amplifies policing.[8] The program is managed by the **Federal Emergency Management Agency (FEMA)** and ties federal money for disaster relief—which cities desperately need for hospitals, fire departments, and alert systems—to policing and surveillance systems. This has given corporations a virtually guaranteed, ever-expanding funding stream.

See **Appendix A** for examples of corporations that rely on UASI funding to increase their revenues for policing and surveillance technologies like gunshot detection, Automated License Plate Readers (ALPRs), social media and data analysis, and data sharing networks.

3. UASI grants fund fusion centers, which operate as black boxes of public-private data collection and sharing across the country. Some of the same corporations that sell surveillance technology drove the development of fusion centers and contributed to DHS's reliance on consumer data collection and information sharing.

Our research exposes the role that corporations played in establishing fusion centers in the early 2000s, and demonstrates how UASI funding and corporate influence helps sustain fusion centers today. In the 2000s, corporations like **Microsoft** pushed for fusion centers as a necessary "counterterrorism" response, and built their infrastructure with government agencies, ensuring a continued reliance on their products.[9] **Fueled by corporate interests, fusion centers have become the center of the data broker economy. The centers rely on consumer databases run by Experian, LexisNexis, and its subsidiary, Accurint.[10]**

Almost two decades of research shows that data fusion centers enhance racialized policing, mass surveillance, government spying on social movements, targeting of Muslims, and immigration detention and deportation. Between corporate lobbying and public-private partnerships, the fusion center network has boomed: there are at least 80 fusion centers across the US and its territories today.[11]

4. Corporations sponsor and fund law enforcement associations and think tanks that drive the "counterterrorism" profit cycle by bringing industry and government officials together to shape policy. These associations advocate for more funding for fusion centers and homeland security grants.

Industry-funded law enforcement associations and think tanks have played a critical role in establishing "homeland security" policy rooted in surveillance and militarized policing. Professional associations and think tanks—like the **National Fusion Center Association**, the **National Homeland Security Association**, the **Integrated Justice Information Systems Institute**, and the **International Association of Chiefs of Police**—host annual conferences where they bring together government and law enforcement officials and corporate partners to shape security "solutions," and provide a venue for corporations to market their security products. These same law enforcement associations, bolstered by corporations, then advocate for more "counterterrorism" grant funding.

These associations have industry ties, from their funders to their executive board members, who drive their priorities when lobbying for "homeland security" funding. **These industry-funded associations give corporations legitimacy and an outsized level of influence as active participants in shaping "homeland security" policies that benefit their businesses**.

RECOMMENDATIONS

Grassroots organizations like Muslim Justice League and the Stop LAPD Spying Coalition have long been organizing against the "homeland security" policing machine because of the violence it inflicts on our communities. Building on the report findings and their years of advocacy, we call for immediate action to address the harms of the "counterterrorism" profit cycle.

See the **Conclusion** of the report for an expanded list of recommendations.

Local & State Action

1. To promote true community safety, city and state officials should reject Urban Area Security Initiative funding and instead invest in public services like education, housing, and healthcare.
2. To protect their residents, city and state officials should divest all funding from fusion centers and other surveillance networks in local and state budgets and instead invest those funds in public services.

Federal Action

1. Congress should immediately cut Homeland Security Grant Program (HSGP) funding by 50 percent and separate funding for emergency response and immigration services from the DHS budget, on the path to total divestment.[12]
2. Congress and federal agencies should limit and regulate corporate data sharing and ensure that "homeland security" and "policing" exceptions are no longer used as loopholes for corporations to profit from mass data collection.

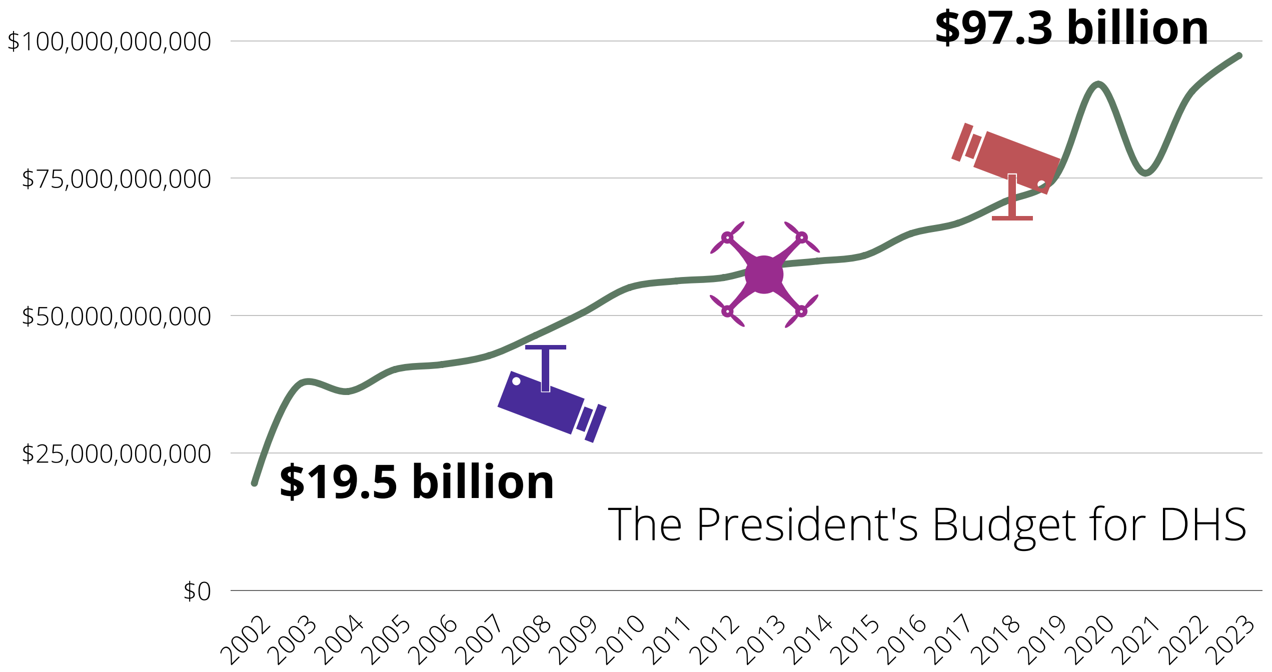
Corporate Action

1. Mass data collection and surveillance should not be profitable, and companies should not be able to make them an essential part of their business model. Corporations like Microsoft, LexisNexis, and Motorola Solutions should not profit off mass consumer data collection, information sharing, and surveillance.
2. Corporations should withdraw funding and sponsorship from law enforcement associations and think tanks pushing "counterterrorism" policies that harm our communities. Corporations like Microsoft, LexisNexis, and Motorola Solutions shouldn't be driving policies that fuel policing in our communities and make a profit from these contracts.
3. Stakeholders of corporations like Microsoft, LexisNexis, and Motorola Solutions—including shareholders, workers, and consumers—can challenge the role these corporations play in exacerbating racist "homeland security" policy and sustaining the "counterterrorism" profit cycle.

INTRODUCTION

Twenty years ago, the Bush administration founded the Department of Homeland Security (DHS) as the heart of the post-9/11 War on Terror. As the Pentagon launched wave after wave of military intervention abroad, DHS entrenched the militarized homeland security state in the United States—targeting Muslims and immigrants. DHS absorbed all federal immigration offices, reframing immigration processing and border control as matters of national security, effectively framing every migrant and immigrant as a potential threat.[13] While the US government has long criminalized immigrants,[14] the founding of DHS supercharged this mission with the rapid infusion of billions of dollars. With this unprecedented budget, DHS drastically expanded immigration policing, surveillance, and data collection, permanently embedding the War on Terror into policing in our neighborhoods.

The War on Terror launched an emergency response that fundamentally transformed immigration and local policing in the United States. The government used the emergency narrative to mobilize billions in funding and evade responsibility for civil liberties and human rights violations globally and locally. **Twenty years later, this state of emergency has not only become permanent, but also incredibly lucrative for big business at the expense of our communities**. The DHS annual budget ballooned from **$19.5 billion in 2002** to almost **$100 billion in 2023**,[15] much of it spent on contracts with corporate partners. Since its founding, DHS has spent an estimated $333 billion on the agencies that carry out immigration enforcement alone—vastly more than any other federal policing agency.[16]



To justify this spending, DHS constructs the idea that the nation is under constant threat. Over the years, the department has continually recreated that threat. DHS functionally intertwines the War on Immigrants, the War on Terror, and the ongoing War on Drugs, which targets and criminalizes Black and Brown communities.[17] In 2002, the Bush administration established the NSEERS program (National Security Entry-Exit Registration System), an Islamophobic "Muslim registry" that required men and boys over the age of 16 from 24 Muslim-majority countries (plus North Korea) to register with immigration authorities; according to DHS, the program funneled over 13,000 into deportation proceedings.[18] In the following years, Immigration and Customs Enforcement (ICE), a new agency under DHS, built up a massive immigration enforcement and deportation operation, targeting immigrants more broadly but relying on the same homeland security justifications. And as the police state and the homeland security machine have become even more entangled, DHS has also collaborated in surveilling Black Lives Matter protesters and other activists.[19]

Corporations like Microsoft, **LexisNexis**, **and Motorola Solutions played an integral role in creating and engineering the homeland security state which helped grow their revenues.** The rapid founding of DHS directed billions to be spent on national security, and gave industry players the chance to drive the department's strategy and operations.[20] The crisis moment of 9/11 presented an opportunity to many of the same corporations that were facing a recession. Corporations pushed government officials towards tech-based "solutions" to their national security concerns, marketing their products—sometimes using Islamophobic tropes[21]—and relying on public safety messaging to justify massive spending on surveillance technologies.

This report reveals how DHS and corporations work to sustain the emergency narrative and expand surveillance and militarized policing at the local and state levels, through counterterrorism grant programs. Every year, DHS allocates hundreds of millions of dollars in counterterrorism grants to local and state agencies across the country, with the requirement that the money is partially used for policing and surveillance technology. DHS's **Homeland Security Grant Program (HSGP)**, and its largest program the **Urban Area Security Initiative (UASI)**, provide millions in additional funding to already bloated police budgets across the country. HSGP and UASI boost police departments' budgets for militarized technology and equipment in the name of counterterrorism and safety.[22] **DHS has awarded almost $28 billion in counterterrorism grant funding since the start of the program.[23]**

In 2021, Crescendo's *Big Tech Sells War* report revealed the rapid growth in revenue that Microsoft and other tech corporations have enjoyed as a result of cloud computing and other technology contracts to support the global War on Terror.[24] ACRE's *21st Century Policing* report from earlier that year highlighted how surveillance vendors like ShotSpotter and Motorola Solutions make millions in contracts with local police and have dangerously expanded the unchecked scale of policing through technology.[25] This report, *DHS Open* *for Business*, reveals how many of the same corporations help sustain War on Terror policies and federal funding for counterterrorism, intensifying systems of surveillance and state violence targeting Muslims, Black, Brown, Asian, Indigenous, and immigrant communities, from the federal to the local level.

Many of the corporations named in this report market themselves as working for the public good, providing products such as computer software, research databases, and communications technology. However, these corporations collectively make billions in revenue through DHS and government contracts for militarized policing technology, invasive surveillance systems, and databases that monetize our most intimate information. Like so many government-constructed wars, such as the War on Drugs and the War on Immigrants, the War on Terror has proven to be a reliable source of profits for corporations, with significant costs to communities.

Together, DHS and these industry partners have not "secured the homeland," but instead have violently intertwined counterterrorism with militarized policing and surveillance systems across the country. In **Section I** of this report, we show how corporations were integral to DHS from the department's inception. In **Section II**, we reveal our findings on how DHS counterterrorism grant programs, specifically UASI, militarize policing and benefit corporations. In **Section III**, we describe the role that data fusion centers, funded by UASI and bolstered by corporations, play in bringing the War on Terror to our neighborhoods. In **Section IV**, we profile industry-funded law enforcement associations which sustain the counterterrorism profit cycle. Finally, the **Conclusion** builds on our findings and years of work by grassroots organizations fighting against the homeland security industry to provide recommendations for organizers and policymakers at the local, state, and federal levels.

I. CORPORATIONS FUEL DEMAND FOR "HOMELAND SECURITY"

"Many companies that rode the dot-com boom need to find big new sources of income... If we have a big federal push for new security spending, that could prop up the sagging market."

- Peter Swire, Ohio State University Law Professor, 2002[26]

Corporations were central to the US government's response to 9/11 and the construction of the Department of Homeland Security (DHS). Faced with a desperate need for revenue after the dot-com bubble burst, many companies capitalized on an opportunity to recover from a recession by signing up to build out mass surveillance infrastructure through homeland security government contracts. **The cycle of counterterrorism profit starts here: corporations fueling the demand for homeland security technology which helps them create a virtually guaranteed revenue stream from government contracts and public funding.**

When the dot-com bubble burst in the early 2000s, commercial and consumer demand for tech services thinned out and the tech industry faced an economic slowdown.[27] Government spending, in contrast, presented a new opportunity for revenue in the aftermath of 9/11: to build infrastructure for an agency that would meet the desire for homeland security and expand the powers of existing agencies.[28] Tech companies of all sizes took on this opportunity to make up for their lost revenues in the recession, and began marketing their technologies to the new department.[29] They succeeded; post-9/11, the increased demand for contracts with technology vendors far outpaced demand for traditional military contractors like Raytheon.[30]

Some corporations also helped shape public sentiment that normalized the need for surveillance in response to 9/11. For example, Siebel Systems, a data-sharing and management company, led a multi-million dollar ad campaign to market its technology as necessary to fight terrorism.[31] In addition to directly lobbying the government for contracts, the company took out ads promoting their products with fear-mongering and Islamophobic tropes, likely aiming to increase public support of expanded surveillance systems. Its full-page newspaper ad read "Who Are the Mohammed Attas of Tomorrow?" with a blurry picture of Mohammed Atta, one of the 9/11 plane hijackers, passing through airport security in Portland, Maine. The ad implies that Siebel's technology would have stopped him.[32]

Corporations Shaped Homeland Security Policy from the Start

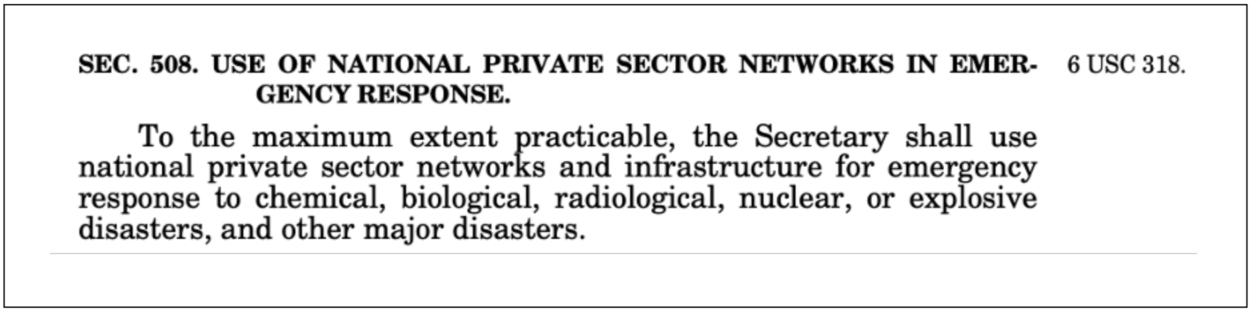
Even before DHS was founded, **corporations were at the homeland security policy**

Source: Photo by Mark Wilson/Getty Images

table, in discussions and working groups with government officials charged with decision-making on national security. In March 2002, President Bush established the first Homeland Security Advisory Council (HSAC) to advise government officials responsible for building new infrastructure in response to 9/11. HSAC consisted primarily of business executives, consultants, and law enforcement representatives.[33] Corporate interests helped shape the council and the very foundation of the homeland security project; in fact many of those represented on the HSAC advocated for policies and contracts that directly benefited their business.[34]

Law enforcement associations, backed by industry players, also played a role in pushing for the establishment of DHS. For example, the International Association of Chiefs of Police (IACP), an association of local and state law enforcement officers, put out a resolution in November 2002 calling on Congress to "pass the necessary legislation to create the Department of Homeland Security" and "provide state and local law enforcement agencies the funding necessary to achieve wireless communication interoperability."[35] As discussed in Section IV, IACP is heavily backed by corporate sponsors, many of which sell policing and surveillance technologies.

The role of the private sector was thus embedded into the founding of DHS. In November 2002, the Homeland Security Act established DHS, which explicitly named the role of private sector networks in emergency response.[36] The text of the bill also called for government agencies to utilize "off-the-shelf commercially developed technologies" in order "to avoid competing commercially with the private sector," further cementing the central role of corporations in DHS's activities and mission.[37]



SEC. 508. USE OF NATIONAL PRIVATE SECTOR NETWORKS IN EMERGENCY RESPONSE. 6 USC 318.

To the maximum extent practicable, the Secretary shall use national private sector networks and infrastructure for emergency response to chemical, biological, radiological, nuclear, or explosive disasters, and other major disasters.

Excerpt from Homeland Security Act of 2002.

The Race for Homeland Security Funding

> *"Software companies looking for greener pastures are turning to the red, white & blue."*
>
> - Alorie Gilbert, writing for business technology news website, ZDNet, 2002[38]

Tech companies aggressively advocated for homeland security as a new source of funding. The newly formed Department of Homeland Security received thousands of proposals from private corporations, particularly software companies, as soon as it was established, to the point where the agency did not even have the staff to be able to review them. Steve Cooper, Chief Information Officer for DHS in 2002 said, "We can't move as fast as we'd like because of the sheer volume, and we don't have enough staff to move as quickly."[39] Corporate lobbying also boomed; at the start of 2002, 157 companies registered lobbying activities around homeland security or counterterrorism, increasing to 569 companies by April 2003.[40]

In 2003, as the department fully began its operations, corporations turned their attention to Tom Ridge, the newly appointed Secretary of Homeland Security.[41] Secretary Ridge was already known to be friendly with tech corporations during his tenure as Governor of Pennsylvania, when he frequently facilitated contracts with Microsoft for government services and sponsored tech-friendly legislation.[42] Corporate executives pursued Ridge through lobbying meetings, public messaging, and at law enforcement conferences. For example, Microsoft CEO Bill Gates met with Ridge in July 2003, lobbying for DHS to use Microsoft's technology. Two days after the meeting, **DHS awarded Microsoft the first technology contract** for the department, a $90 million desktop and server infrastructure contract for 140,000 users at the department.[43]

Motorola Solutions, a communications technology and data analysis software provider that receives millions in DHS grant funding today, was also present in this early period. Gregory Brown, then President and CEO of Motorola's Commercial Government and Industry Solutions Sector, testified at a June 2003 Congressional hearing about the importance of "communications interoperability" for law enforcement. His testimony specifically mentioned how DHS could provide funding for this technology to cities and states through homeland security grant funding,[44] which will be discussed in Section II. Motorola's lobbying profile in the years following 9/11 also notes activity focused on homeland security, disaster and emergency planning, and immigration.[45] Motorola Solutions advertised their homeland security opportunities to investors in financial documents, noting that the "our business is well positioned to participate in [the] emerging opportunity" of the federal government's post-9/11 strategy.[46]

LexisNexis and other companies promoted their information technology services as a new "weapon" in the War on Terror, providing the tools for the government's racial profiling of Arab and Muslim men.[47] After 9/11, a LexisNexis risk management team volunteered its services to the FBI.[48] LexisNexis provided its SmartLinx[49] database to the FBI to investigate Khalid Al-Draibi, a Saudi man working in the United States as a cabdriver, after police detained him in Virginia on September 11th for driving with a flat tire and falsely accused him of involvement in the attacks.[50] LexisNexis's SmartLinx contributed to the FBI's continued profiling and detention of al-Draibi—who was later cleared of terrorism accusations but still detained and deported under immigration-related charges.[51]

Source: JHVEPhoto/Shutterstock.com

LexisNexis highlighted its role in the Al-Draibi case in later publicity pitches for its SmartLinx product,[52] and simultaneously sponsored research and wrote policy papers with findings that called for services that the company could provide. LexisNexis funded multiple studies on identity fraud in the early 2000s to motivate federal investment.[53] In 2003, they published a paper calling for federal funding to combat identity fraud through domestic and global data sharing networks.[54] Today, LexisNexis states it has data contracts with 70 percent of local agencies and almost 80 percent of federal agencies.[55]

Industry coordination also played an important role in this funding race. For example, the Armed Forces Communications and Electronics Association (AFCEA) hosted conferences for corporations to meet government officials and market their technologies in the years immediately following 9/11.[56] ManTech International, the first company to contract with DHS for the Homeland Security Information Network (HSIN), was one of the exhibitors at these early conferences.[57] Today, the HSIN is the official information sharing database between DHS and other local, state, and federal agencies, and hosted on Amazon Web Services.[58]

The IACP, mentioned above and outlined in further detail in Section IV, also hosted a conference in October 2003 with law enforcement officials from DHS and the Department of Justice alongside corporations marketing their homeland security technologies.[59] Corporate attendees included data mining companies like **i2**, facial recognition technology vendors like **Verint Systems**, and data brokers like **LexisNexis**, as well as **ChoicePoint** and **Seisint**, which LexisNexis's parent company would later acquire.[60]

Microsoft, Motorola Solutions, and LexisNexis, like many other corporations, not only took advantage of funding opportunities from the federal government, but also lobbied government officials to sell their technologies as counterterrorism solutions. This corporate role shaped how the new department responded to "threats of terrorism," developing DHS's dependence on consumer technology and data as the anchor for counterterrorism operations, immigration policing, and surveillance.

Revolving Doors, Influencing Strategy, and Securing Contracts

Tech companies like Microsoft embedded themselves in this newly created homeland security ecosystem. Microsoft appointed Thomas Richey, former security advisor to John Kerry, as the company's first Director of Homeland Security only one year after 9/11.[61] Richey developed Microsoft's strategy to collaborate with the federal government on homeland security and led working groups for Microsoft executives and DHS officials to co-create homeland security policy.[62] Gates and Richey also both participated in public events that brought together industry and government officials to talk about the role of technology in homeland security.[63]

> *"Tom [Richey]'s appointment is a significant step in establishing Microsoft as a strategic partner to the government as it evolves its homeland security strategy,"*
>
> \- Mitra Azizirad, general manager of Microsoft's federal systems[64]

Around the same time, Howard Schmidt, the former Chief Security Strategist at Microsoft, was appointed the Vice Chairman of the President's Critical Infrastructure Protection Board (CIPB) created in October 2001.[65] The CIPB was responsible for the "National Strategy to Secure Cyberspace," a plan that Schmidt became well known for and that highlighted the role corporations could play in the government's cybersecurity initiatives.[66] Today, Microsoft remains a key player in cybersecurity policy and a main contractor for government IT infrastructure.[67]

IN A 2004 INTERVIEW, THOMAS RICHEY SAID

“Our #1 goal at Microsoft is to help the president, the Secretary of Homeland Security. . . achieve all their goals around homeland security. . . So they've made a significant investment in us and in turn we've made a significant investment in their success. ”

As DHS moved into a fully operational phase, the revolving corporate door continued to spin. In 2003, Microsoft hired Michael Byrne, only a few months after he started his role in the nascent DHS Office of National Capital Region Coordination to enhance collaboration across federal, state, and local governments.[68] At Microsoft, he took the role of Director of Justice and Public Safety, where he helped "mayors, police chiefs, and other first responders close the

technology gaps in record-keeping systems and databases."[69] This role almost directly mimicked his government job, strengthening information sharing and collaboration, but with Byrne now tasked with selling Microsoft's technology to achieve the mission.

Today, Microsoft is a central cloud computing provider to DHS and other policing agencies across the federal government; and between 2011 and 2020, the company secured over $266 million in contracts with DHS, not including its contracts with local and state policing agencies.[70] Microsoft regularly partners with local police departments to build up their surveillance capabilities, through projects like the Domain Awareness System in New York City,[71] which this report describes in Section II.

Similar to Microsoft, LexisNexis ramped up its homeland security business operations post-9/11 with the focus on fraud, identity, and consumer data, intensifying a shift from its origins in legal research and journalistic information services.[72] This set the stage for the company to become a key data broker for DHS,[73] with the help of a revolving door of law enforcement personnel.[74]

In 2003, the company founded a subsidiary called **LexisNexis Special Services Inc.** (LNSSI), one example of the corporation's expanding infrastructure to accommodate DHS's increasing demand for consumer data.[75] LNSSI focused on providing government agencies with data analytics capacity for enforcement operations.[76] LNSSI's board of directors includes local, state, and federal law enforcement officials, a fact used to advertise its products as law-enforcement-approved.[77] In 2004, LexisNexis also acquired **Seisint**, the company behind the foundational information sharing system **MATRIX**, which was pitched as a counterterrorism product but in reality was used to expand Islamophobic policing power through mass data collection, unprecedented data sharing, and surveillance.[78] The acquisition spree continued; in 2008, LexisNexis' parent company bought risk management company **ChoicePoint** to "be able to deliver new and innovative tools to aid federal and state law enforcement agencies in their work," as a pivotal investment in the expanding consumer data sharing industry which policing increasingly relies on.[79]

Today, LexisNexis is a key data broker to ICE and DHS, providing data on millions of people to power ICE's deportations.[80] As outlined in *Who's Behind ICE?*, many of the same tech and surveillance companies targeted in this report have simultaneously boosted ICE's ability to track, detain, and deport immigrants.[81] Organizations like Mijente, the Surveillance, Tech, and Immigration Policing Project at the Immigrant Defense Project, and Just Futures Law have been actively campaigning against LexisNexis, which took on contracts with ICE in 2021 after previously downplaying any collaboration.[82]

LexisNexis and Microsoft are central to DHS policing and surveillance systems, through contracts that help target Black, Brown, Asian, and immigrant communities and increase corporate revenues. These companies worked with DHS to develop its early technology systems, and have become the backbone of the department's cloud computing, data collection and sharing, and surveillance technologies today.

Dodging Regulation In the Name of Homeland Security

Companies also used the homeland security crisis to advance their own policy goals and shape regulations that could limit their business operations. While corporations were lobbying DHS to create demand for their counterterrorism products, they simultaneously invested in molding privacy and civil liberties regulations.

After 9/11, the drive for homeland security fueled the expansion of the data broker industry, now one of the most dangerous actors in the expanding surveillance and data economy.[83] Data broker firms like LexisNexis and Thomson Reuters collect vast amounts of people's intimate personal data, including from phone, electricity, and Internet companies, DMVs, public property records, and health records. They then package and sell this data, often to law enforcement agencies, usually without the knowledge of consumers.[84]

In April 2002, the Center for Information Policy Leadership (CIPL), an industry-backed think tank, brought together Experian, Visa, Fidelity, and thirteen other companies to discuss the role consumer data could play to "create profiles about what a bad guy might look like" and respond to terrorism.[85] A circulated CIPL memo outlined priorities for the organization including combating privacy protection legislation.[86] In the years following the founding of DHS, CIPL played an important role in privacy debates, consulting with DHS and the federal government on issues of data mining and publishing research papers on the topic.[87] CIPL, alongside other industry actors including its member LexisNexis, supported weak federal privacy legislation in anticipation of stricter state restrictions,[88] while continuing to justify why its industry members should be allowed to continue to collect and sell personal data.

Tech corporations also pushed for legislation that expanded government surveillance at the expense of civil rights, including the 2001 PATRIOT Act which authorized a broad range of intrusive surveillance powers for the federal government in the name of national security. Microsoft listed the PATRIOT Act on its lobbying disclosures.[89] Verint Systems, a facial recognition company, boasted the benefits of shifting regulation through the PATRIOT Act for business.[90] The CEO of a facial recognition technology vendor, Visionics, later testified to Congress in November 2001 about the need to institute its technology for security at airports, adding that regulation can happen in "due time" and that Congress should remain "focused on the real and present danger of terrorism and not the theoretical potential for misuse down the line."[91]

While we might expect that corporations were competing for contracts, they often worked together to create favorable legislative conditions to increase their revenues. Today, many of the corporations that contract with DHS sponsor the various industry-funded law enforcement associations that push back against data privacy regulation. Shaping regulation and securing government contracts are not separate goals—corporations rely on lax regulation to contract with policing agencies for profit.

No DHS Without Corporations

Corporations were key partners in imagining and carrying out the vision of the Department of Homeland Security, from strengthening the demand for their services, to hiring government officials as their executives, to lobbying to protect their homeland security revenues. **Without corporations, there is no Department of Homeland Security.** Corporations' role in fueling homeland security policy is only the first leg of the counterterrorism profit cycle. Section II will outline how corporations benefit from the demand they helped create for counterterrorism products at the local and state levels.

II. DHS GRANTS EXPAND THE GLOBAL WAR ON TERROR TO OUR CITIES

DHS framed its programs and funding following 9/11 as an emergency response to disaster. This allowed the department to justify its surveillance and targeting of Muslims and immigrants after 9/11 and avoid accountability for its human rights violations. As with the framing of public safety, which is often used to justify militarized and racist policing, homeland security and emergency response similarly obscure how the federal government and their contractors criminalize targets of the War on Terror, in favor of words that sound much more objective.

Though images of the War on Terror may remind us of the Pentagon and military intervention, DHS and the 9/11 response also had a deep impact on expanding policing in our neighborhoods. Our findings reveal how DHS counterterrorism funding to local and state agencies extends the War on Terror from the federal to community level. We show that corporations not only helped fuel the initial demand for homeland security products, but also continue to promote and benefit from the DHS funding streams at the expense of our communities.

> As one homeland security threat (natural or man-made) is identified and met, other threats develop and require new homeland security capabilities or processes.”
>
> - CONGRESSIONAL RESEARCH SERVICE (CRS) REPORT ON EMERGENCY MANAGEMENT[92]

The Homeland Security Grant Program (HSGP)

The Homeland Security Grant Program (HSGP), DHS's flagship grant program, exemplifies this emergency mission by driving federal funding to local and state agencies to prepare for and respond to "acts of terrorism and other threats."[93] The grant program was established in 2002, almost immediately after the passage of the Homeland Security Act of 2002, which founded DHS.[94]

In reality, HSGP funds policing agencies to buy surveillance technology, expanding the War on Terror to the neighborhood level. **In 2022 alone, DHS awarded $1.12 billion in funds as part of the HSGP, awarding almost $28 billion since the start of the program in 2002.[95]** HSGP relies on the frame of emergency response to provide additional funding to already bloated police budgets.

$28 BILLION

FROM 2003 TO 2022

Urban Area Security Initiative

State Homeland Security Program

Operation Stonegarden

The Role of the Federal Emergency Management Agency (FEMA)

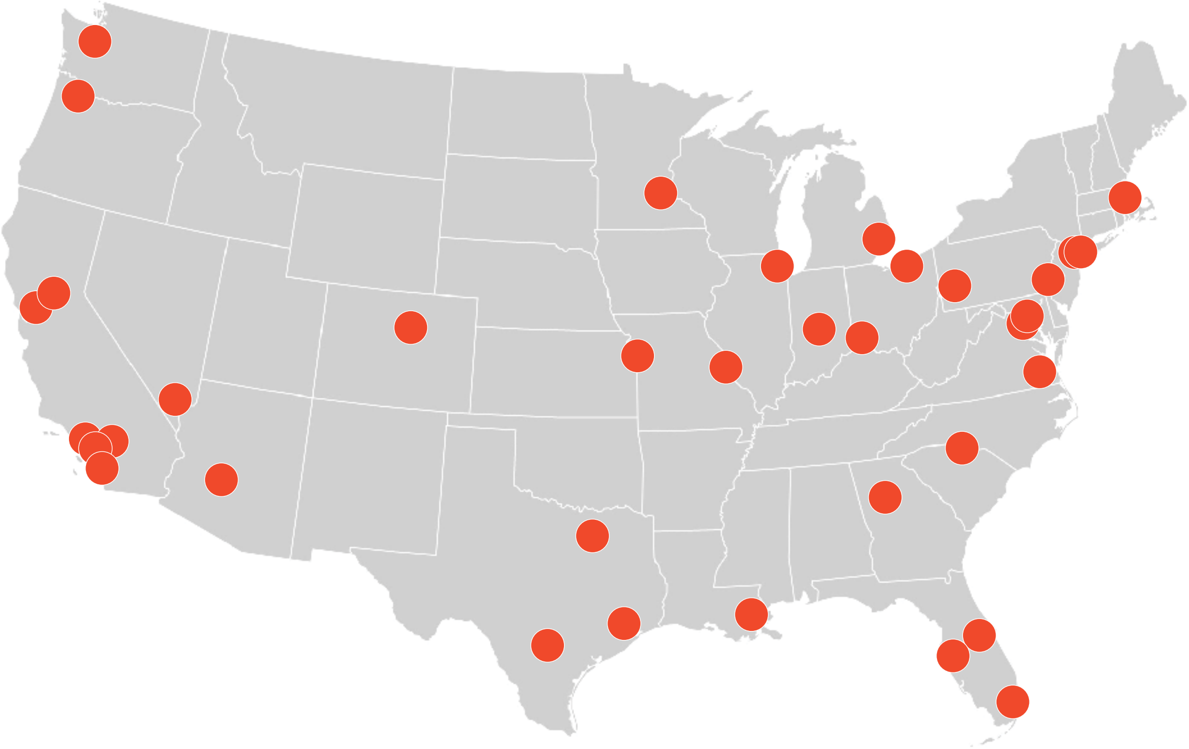
The HSGP is operated by the Federal Emergency Management Agency (FEMA),[96] which was established in 1979 as an independent agency, and then incorporated into DHS when the department was founded in 2002.[97] This placed FEMA's mandate to coordinate disaster response under a national security mission. **Embedding the counterterrorism grant program under FEMA effectively tied federal money for disaster relief and preparedness to funding for surveillance and policing**. HSGP funds and manages three grant programs that expand the national security mission to jurisdictions across the country: the Urban Area Security Initiative (UASI) and the State Homeland Security Program (SHSP), both of which fund local, state, and tribal counterterrorism activities and strategies, and Operation Stonegarden (OPSG), which enhances coordination between immigration enforcement and local police.[98]

In addition to funding equipment and programs for local disaster response and law enforcement, UASI often funds emergency management offices themselves. This makes localities further dependent on counterterrorism funds to respond to climate crises and other disasters. For example, 37% of New York City's Emergency Management department's preliminary 2023 budget comes from federal funding, almost all of which is UASI funding.[99]

In addition to HSGP and other grant funding, FEMA is also responsible for the Countering Violent Extremism (CVE) program, which is known today as Targeted Violence and Terrorism Prevention (TVTP).[100] This program claims to "steer people off pathways to 'radicalization' or 'extremism,'"on the basis of arbitrary factors and unscientific theories of radicalization.[101] The program recruits community members as informants for surveillance, often using mental health as a justification for reporting someone supposedly at risk of violence. Numerous reports and organizing efforts by groups like Muslim Justice League have illuminated how these programs almost always target Muslims and communities of color,[102] and falsely legitimize discrimination against Muslims and other communities that policing agencies frame as "inherently violent."[103] Both CVE and HSGP programs exemplify how DHS has entrenched FEMA at the center of the domestic War on Terror, using the language of threats and states of emergency to expand policing.

The Urban Area Security Initiative (UASI)

Today, the Urban Area Security Initiative (UASI) is the largest program of the HSGP. **UASI has provided billions of dollars in funding to local and state agencies in "high threat" areas across the country**, defined by DHS as areas with the highest likelihood of terrorism.[104] Most recently in 2022, UASI awarded a total of **$615**



The 36 metropolitan regions that received UASI funding from DHS in 2022

million to **36 metropolitan areas**.[105] **This report focuses on UASI grants as an example of how federal funding fuels local policing, and who the corporate profiteers are**.

UASI grants are first disbursed to coordinating entities at the state level, which then allocate funding to specific cities.[106] **According to DHS requirements, cities cannot receive any grant funding under UASI unless they specifically allocate a set portion of their funds to law enforcement activities.[107]** Beginning in 2007, DHS mandated that a minimum of 25% of funding go towards law enforcement activities, which can include "domestic violent extremism," intelligence, cybersecurity, information sharing, and other outlined DHS priorities. In 2022, that requirement was increased for the first time to 30%, indicating a message to local and state agencies that policing is an increasingly central priority.[108]

UASI's other funding categories include emergency preparedness and disaster equipment, such as city-wide emergency alert systems, funding to hospitals, and funding for fire departments.[109] Under DHS and FEMA, some of these emergency and disaster response systems are also increasingly intertwined with policing; for example, some UASI-funded emergency alert systems are shared with police departments.[110] And while many of these services are essential to disaster response, none should be tied to militarized policing—neither for funding nor data sharing.

More DHS funding for law enforcement means more funding for data fusion centers. As discussed in Section III, fusion centers are massive hubs of information sharing between local, state, and federal agencies and corporations that operate with little oversight. This data sharing focuses on the intimate personal information of millions of people, making it easier for law enforcement to use our personal data to target and criminalize our communities.

UASI grants marked for law enforcement must be spent on authorized equipment as defined by DHS.[111] This authorized equipment includes invasive surveillance technologies like license plate readers, gunshot detection technology, social media surveillance technology, and drones. The equipment list also includes radio systems, communication interoperability, "bomb robots" used to dismantle bombs without human contact, militarized policing equipment, and physical infrastructure like barriers and armored vehicles.[112]

UASI funding is also authorized for law enforcement trainings, which may sound benign or positive but have included trainings that attempt to emulate "terrorist attacks" with flagrantly Islamophobic tropes. Some of these trainings, which are often administered by an outside vendor, demonstrate how corporations amplify federal officials' and law enforcement's anti-Muslim sentiment. For example, UASI-funded company Security Solutions International (SSI) has offered trainings with modules and conferences titled "The Islamic Jihadist Threat" and "Allah in America."[113] According to analyses by Political Research Associates and the Council on American Islamic Relations, the content of these sessions stokes fear of Muslim communities in trainings for law enforcement.[114]

HOW ARE COMMUNITIES PUSHING BACK AGAINST UASI?

Communities across the country have campaigned against UASI for years, targeting fusion centers, surveillance technology, and militarized policing. These include:

Muslim Justice League, a grassroots organization in Boston representing Muslim community members in the city, has been campaigning against the Boston Regional Intelligence Center (BRIC), the main UASI-funded fusion center in Boston.[115]

Stop LAPD Spying, a Los Angeles-based coalition working towards abolishing police surveillance, has campaigned against the UASI-funded Joint Regional Intelligence Center (JRIC) in Los Angeles.[116]

In 2019, a coalition of community organizations led by the **War Resisters League** targeted UASI in a successful campaign to force Oakland to decline hosting Urban Shield, a surveillance and weapons exposition that was funded by UASI.[117]

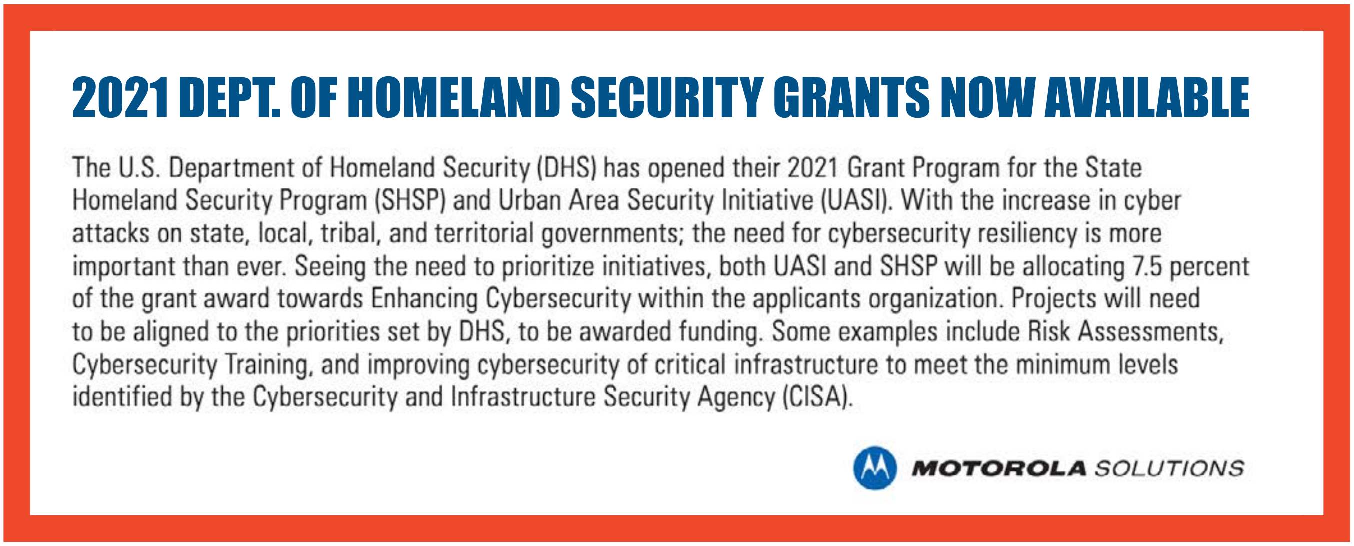
Companies Market Their Technology for UASI Use

Seeing the potential revenues in the post-9/11 federal budget, many corporations focused on UASI funding as a key target. **Our research shows that corporations are entwined in the UASI funding process** by marketing their products and UASI funding streams to local officials, direct lobbying for increased federal funding, and support for law enforcement associations. These activities produce results for corporations: state and local agencies use UASI funds to contract with Motorola Solutions, Microsoft, Dataminr, Skopenow, Palantir, ShotSpotter, and many other corporations that sell surveillance, policing, and data collection technologies.

Many of these companies actively advertise their products as eligible for UASI funding, in their public materials and interactions with local and state officials, and **even support the grant application process.** Motorola Solutions and ShotSpotter, for example, put out informational materials and regularly host webinars for local officials about how to take advantage of DHS grant funding to purchase surveillance technology.[118] Companies including **Motorola Solutions** partner with and sponsor services like PoliceGrantsHelp.com, which make it easier for police departments to apply for grant programs like UASI to buy their technology for policing.[119]

At the same time, these corporations lobby the federal government to maintain and expand funding, in order to secure their revenue streams. Motorola Solutions's lobbying profile indicates lobbying on "FY23 Department of Homeland Security Appropriations" as well as other appropriations bills for federal policing agencies.[120] Microsoft also lobbies on federal appropriations bills, including the "Consolidated Appropriations Act of 2022," which includes funding for the Department of Homeland Security.[121]

These companies also promote their technologies at conferences for law enforcement associations. These include the National Homeland Security Association, which was founded to bring together local homeland security officials from different regions, and strongly promotes public-private partnerships and collaborations with technology vendors.[122] Section IV of our report dives further into how these industry-backed associations operate and the role they play in the homeland security ecosystem.



2021 DEPT. OF HOMELAND SECURITY GRANTS NOW AVAILABLE

The U.S. Department of Homeland Security (DHS) has opened their 2021 Grant Program for the State Homeland Security Program (SHSP) and Urban Area Security Initiative (UASI). With the increase in cyber attacks on state, local, tribal, and territorial governments; the need for cybersecurity resiliency is more important than ever. Seeing the need to prioritize initiatives, both UASI and SHSP will be allocating 7.5 percent of the grant award towards Enhancing Cybersecurity within the applicants organization. Projects will need to be aligned to the priorities set by DHS, to be awarded funding. Some examples include Risk Assessments, Cybersecurity Training, and improving cybersecurity of critical infrastructure to meet the minimum levels identified by the Cybersecurity and Infrastructure Security Agency (CISA).

2021 Motorola Solutions advertisement for DHS grant funding.

UASI Funding Across Four US Cities

> *"So I ask you, no matter where you come from: take bold action to ensure the safety of cities across our nation and fully fund UASI. This is tantamount to protecting not just the safety and economic vitality of New York City, but that of our region and the nation as a whole."*[123]
>
> - Former Mayor of New York City, Bill DeBlasio, testifying to Congress in 2016

In order to understand how UASI grant funding is spent across the country, we, alongside partners like Muslim Justice League and American Friends Service Committee, submitted records requests in early 2022 to officials in Los Angeles, New York City, Chicago, and Boston. We selected these cities because they are some of the largest recipients of UASI funding. These records requests were directed to local police departments, state and local offices of emergency management, and other public safety departments. Unfortunately, multiple agencies did not respond to our records requests or directly rejected them under exemptions regarding national security. Law enforcement and national security exemptions have long been a way for policing agencies to use a "security" excuse to evade transparency and accountability.[124] We supplemented the documents we did receive with an analysis of industry materials, local budgeting and city council records, and federal reports.

Our analysis found that in these cities, many of the same corporations that lobbied for increased federal funding receive millions in UASI funding for surveillance technology. This effectively increases local policing agencies' budgets, specifically for these corporations' projects, while letting both avoid the same level of oversight as local procurement processes. **As we outline in detail below, cities frequently used UASI funds to purchase invasive surveillance technologies and militarized police equipment**.

ShotSpotter®

Gunshot detection technology: In the Boston region, **ShotSpotter** contracts across Cambridge, Chelsea, Somerville, and Boston have been paid for by UASI funding for almost a decade, rather than pulling from the police or other city department budgets.[125] Other cities including San Jose and Miami Gardens also relied on UASI funding for ShotSpotter.[126] Though our research focused on four cities, there are likely many more localites that rely on UASI funding to pay for ShotSpotter's gunshot detection. Gunshot detection technology, which attempts to dispatch police whenever a "gunshot sound" is heard, can often be faulty, has led to police murder and false arrests, and increases police presence in our neighborhoods.[127]

Automatic License Plate Readers (ALPRs): UASI funding also frequently paid for automatic license plate reader technology, which allows police and ICE to track vehicles' movements historically and in real-time. ALPR data can reveal intimate information about where we live, work, travel, protest, worship, and seek legal support or healthcare. Between 2016 to 2020, Los Angeles budgeted at least $1.27 million on license plate reader technology, likely comprising its contracts with **Vigilant Solutions**.[128] In Cook County, which is part of the Chicago UASI region, ALPR device and ALPR data purchases from Vigilant Solutions showed up in UASI vendor quotes submitted by local police departments for approval.[129] In Boston, UASI funding also paid for license plate readers.[130]

Radio communications technology: Funding radio through UASI is another boost to policing budgets. Radio communications can also allow police to avoid public oversight, as was the case in California when police blocked journalist access to their radio systems.[131] Between 2016 to 2020, Los Angeles Police Department (LAPD) budgeted over $24 million in UASI funds for upgrading its radio systems, which have historically been provided by **Motorola Solutions**.[132] In 2016, Chicago signed a five-year $25 million contract with Motorola Solutions paid in UASI funds.[133] Cook County's UASI vendor quotes also included a quote from Motorola Solutions.[134] In Boston, UASI funding also paid for radio system upgrades.[135]

Predictive policing technology: In Los Angeles, UASI funding was used to pay for **Palantir** "advanced data fusion platform" licenses for the LAPD.[136] These Palantir licenses are likely connected to the company's partnerships with LAPD which amass large amounts of personal data and analyze it to determine future "crime hot spots."[137] This practice is known as predictive policing, which unscientifically relies on biased police data to "predict" future crimes and reinforces the policing of Black and Brown neighborhoods. Palantir, in particular, has played a key role in ICE's deportation machine.[138]

Social media surveillance technology: In Los Angeles, 2020 UASI funding was used to pay for a software license with **Skopenow**, a social media data mining and surveillance company.[139] In New York City, UASI funding was used to pay for Dataminr social media monitoring contracts.[140] **Dataminr** is a data broker and social media surveillance company that has helped police monitor communities of color and Black Lives Matter protests, reportedly with blatant racial profiling tactics.[141] Social media surveillance technology allows police access to intimate personal information and build "networks," like gang databases—which attempt to build affiliation between community members and those who are targeted by police—to criminalize speech, protest, and association.

Cell site simulators: Also known as "stingrays," cell site simulators are invasive surveillance devices that trick cell phones in the area into sending their locations, identifying information, and even call and text information.[142] In Los Angeles, 2020 UASI funds paid almost $630,000 for a cell site simulator system, including training.[143] Advocates have also uncovered that UASI grants have funded cell site simulators for police departments in other cities, including Anaheim, Alameda, San Francisco, San Jose, and Oakland.[144]

Surveillance and data sharing networks: In addition to specific surveillance technologies, UASI funding has long helped cities build and sustain massive surveillance systems and data sharing networks, which equip police to monitor city residents 24/7. This expands both indiscriminate mass surveillance of millions of people and targeted surveillance that criminalizes specific individuals.[145] In New York City, **Microsoft** custom-built the Domain Awareness System (DAS), a 24/7 live feed of surveillance data for the New York Police Department (NYPD), with almost $400 million in UASI funding.[146] Launched in 2012 as a "counterterrorism" measure, DAS supercharges everyday policing, compiling real-time surveillance data from across the city, including license plate readers, gunshot detection devices from ShotSpotter, CCTV cameras, and predictive policing software.[147] In Boston, the Critical Infrastructure Monitoring System (CIMS) project, also funded by UASI, plays a similar role, bringing together surveillance data from camera networks across the region. CIMS uses analytical services from company **BriefCam**, which identifies people and shares invasive surveillance data across cities.[148]

Law enforcement training: UASI dollars are also funneled into trainings with many of the companies already providing policing and surveillance technology, adding an additional revenue stream for these corporations. In Los Angeles, UASI funding covered $230,000 in costs for LAPD's participation in the "Leadership in Counter-Terrorism Conference" in 2016, 2017, and 2020.[155] The program, which is jointly run by the FBI, includes Palantir as a corporate partner of its association.[156] The LAPD simultaneously used UASI funds to pay for Palantir's services, allocating an estimated $1.4 million on training

A DEEPER LOOK AT UASI'S ROLE IN THE NYPD'S DOMAIN AWARENESS SYSTEM

In 2012, the NYPD and Microsoft jointly announced their partnership to build the Domain Awareness System (DAS),[149] which as of 2021 was funded by at least $488.8 million in federal homeland security grants, including UASI.[150] It is unclear what percentage of DAS is funded by UASI, but in 2016 then-mayor Bill de Blasio stated that UASI provides the entire budget for DAS.[151] DAS allows the NYPD and its federal partner agencies to monitor New Yorkers in real time, all while furnishing millions in revenue to Microsoft, with little information shared with the public.

Microsoft also sells DAS to other police departments, with the NYPD receiving 30 percent of revenues from those sales.[152] While city and state officials lobby for this funding with counterterrorism rhetoric,[153] in reality, DAS has reportedly been used to target Black and Brown New Yorkers and is of increasing concern to public defenders and immigrants rights groups in the city.[154]

and its "advanced data fusion platform" licenses between 2016 and 2020.[157]

In Boston, UASI funding paid for various emergency preparedness training.[158] In Chicago, several million dollars per year were allocated towards generic "training" as well.[159] Though the documents we received did not specify what type of training the funding was going towards, it is reasonable to guess that the training consisted of mock attack scenarios and orienting intelligence analysts to new technology. A FEMA case study noted that UASI-funded training in Chicago proved effective in responding to "civil unrest" and "large-scale protests" in May 2020, pointing to the city's ability to "extinguish fires" and perform "civil unrest responses" concurrently.[160]

Emergency preparedness systems: As mentioned above, UASI funding is also used for emergency preparedness activities like emergency notification systems in New York City and Boston.[161] These systems sound harmless and necessary but are often intimately tied to surveillance and policing, in addition to their emergency alert or other preparedness functions. For example, New York City's contract with **Dataminr** for social media surveillance mentioned above is held by the City's Office of Emergency Management (OEM).[162] An OEM Records Access Officer wrote in an email that the office shares this contract with the NYPD, which highlights how UASI links emergency response to policing and demonstrates a likelihood that the NYPD shares access to the same Dataminr systems and data as the emergency management office.[163]

Militarized physical equipment: Equipment like vehicle barriers, armored tanks, and SWAT equipment were paid for in at least Los Angeles, Chicago, and Boston regions using UASI funding.[164] While it's unclear whether this equipment has directly been used to suppress protests, FEMA provided testimony in response to questions about the role that UASI-funded equipment may have played in the 2014 uprisings in Ferguson, Missouri. The testimony found that the St. Louis UASI region had received various equipment from FEMA grants that was ultimately utilized in Ferguson.[165] The agency shrugged off real responsibility for oversight by saying it was too difficult to track the exact equipment used against protesters that was UASI-funded.

UASI Grant Funding Allows Corporations to Profit from the War on Terror Locally

DHS, in partnership with local and state police, use **UASI counterterrorism funding as a convenient shield for increased surveillance, militarized policing, and collaboration with corporations.** With their permanent emergency justification, UASI grants incentivize heavy spending on surveillance and policing, and virtually guarantee a revenue stream for the corporations selling these technologies. UASI's corporate partners not only help police departments to increasingly adopt militarized equipment, but as discussed in Section III, enhance the harms of fusion centers, which have consistently targeted Muslims and political protesters across the country—such as those protesting against police violence or for abortion access.[166] Rather than keep people safe, UASI continues to expand the scope of the War on Terror from DHS to the police in our neighborhoods, benefiting the corporations extracting and selling our data.

III. UASI-FUNDED FUSION CENTERS EXPAND THE WAR ON TERROR

"I believe that fusion centers will be the centerpiece of state, local, and federal intelligence-sharing for the future and that the Department of Homeland Security will be working and aiming its programs to underlie fusion centers...And by the way, let's not forget the private sector when we're looking at those partnerships."

- DHS Secretary Janet Napolitano at a fusion center conference, 2009[167]

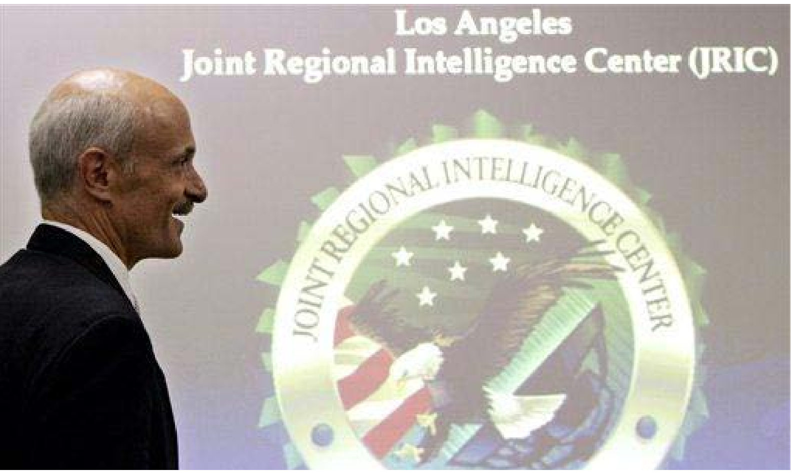
Fusion centers are a key example of how corporations and the federal government collaborate to expand policing, target protestors, and criminalize Muslim, immigrant, Black, Brown, and Indigenous communities. **Our research found that UASI grant funding sustains fusion centers, and that corporations played a pivotal role in creating a fusion center model that allows them to continue to benefit financially from their operations today.**

Understanding the Harms of Fusion Centers

For years, communities and advocates have been calling to shut down fusion centers, which operate as government-run black boxes for mass surveillance. Fusion centers (also called "data fusion centers") are physical sites for information sharing between local, state, and federal government agencies, and their private industry partners. They collect, analyze, and share massive amounts of people's personal data—with little government oversight or public knowledge.[168] This public and private sector data includes surveillance camera networks, telecommunications, facial recognition, controversial private companies' databases and predictive policing software, and government databases.[169] Supported by DHS, fusion centers are operated at the state level or in major urban areas like Los Angeles, Chicago, and Boston.

Fusion centers were founded as part of the post-9/11 counterterrorism response. **In the two decades since, fusion centers have been consistently used to facilitate day-to-day policing, mass surveillance, immigration detention and deportation, and government spying on social movements and activists, including those protesting for abortion access**.[170] A 2012 bipartisan Senate investigation found that fusion centers yield little benefit for federal counterterrorism efforts even as fusion centers are "endangering citizens' civil liberties."[171]

Working with corporate surveillance vendors, fusion centers are central to racial profiling programs, like the Suspicious Activity Reporting programs (SARs), which solicit community reports of "threatening" behavior and overwhelmingly target Muslim communities and people of color.[172] A recent report from the Arab


Los Angeles
Joint Regional Intelligence Center (JRIC)
JOINT REGIONAL INTELLIGENCE CENTER

Secretary of Homeland Security Michael Chertoff moves into place to address the media after touring the Los Angeles Joint Regional Intelligence Center in Norwalk, Calif., Friday, Aug. 18, 2006. (AP Photo/Nick Ut)

American Action Network and the Policing in Chicago Research Group analyzed over 200 SARs complaints from fusion centers in Illinois and found that these complaints disproportionately were unfounded reports targeting Muslim and Arab communities.[173]

Fusion centers harm communities of color, with racist data and algorithms at their core. For example, a Muslim Justice League report on the Boston Regional Intellegence Center (BRIC) found that 97.7% of people in a "gang database" housed within the BRIC fusion center are people of color, and more than 75% of the people in the database are Black men or teens.[174] Fusion centers also give local agencies more power to collaborate with ICE to deport immigrants, often bypassing privacy laws and sanctuary policies which limit information sharing between local and federal authorities to protect immigrant communities.[175]

9/11 to Today: Corporate Influence on Fusion Center Founding, Funding, and Policy

Corporations helped drive the demand for fusion centers and shape the policies behind them—and now they profit from contracts that expand their reach. After 9/11, both industry and government pushed fusion centers as counterterrorism solutions, with the Department of Justice promoting them as essential to "fight crime and terrorism by merging data from a variety of sources."[176]

There were two main waves of fusion center development in the early 2000s. Early discussions about responses to 9/11 focused heavily on information sharing across agencies as a solution.[177] Federal agencies, state governments, and corporations called for fusion centers as the strategy to achieve this mission. Another catalyst for their development was a Homeland Security Advisory Council (HSAC) meeting in March 2005.[178] As discussed in Section I, the HSAC has primarily consisted of business executives, consultants, and law enforcement representatives.[179] In the meeting, the HSAC called for every state to establish a fusion center, and also recommended starting a working group to focus on Homeland Security information sharing with the private sector.[180] **The funding followed**: for fiscal years 2004–2006, DHS homeland security grants directed almost $131 million to states and cities for "fusion-related activities."[181]

In July 2005, the HSAC and the Department of Justice issued the first Fusion Center Guidelines, the foundational document shaping fusion center operations and information sharing.[182] In 2006, they expanded the guidelines to "integrate...private sector entities."[183] By the end of that year, at least 37 fusion centers had begun operations.[184] Since then, the **industry has boomed as the federal government and the private sector invest in the model,** pushing cities and states to simultaneously invest their own resources:[185] **there are at least 80 fusion centers today.[186]**

By design, fusion centers could not exist without corporations. The industry not only invested in creating the fusion center structure, but established key partnerships and contracts to embed their products in fusion center operations. The first fusion centers used data broker **Experian**'s consumer database, in addition to other databases like **Accurint**, a **LexisNexis** product as well as **ChoicePoint**, which LexisNexis acquired in 2008.[187] **Microsoft** collaborated with Illinois State Police to develop key fusion center infrastructure in 2006–2007, at the time called FusionX.[188]

Today, corporations provide the key services that fusion centers rely on: commercial surveillance, data collection, data analytics software, and data management platforms. Private company databases, like those run by **Experian** and **LexisNexis** subsidiary **Accurint**, give fusion centers access to profiles of hundreds of millions of people, using data mined from a range of public and private sources; this includes people's identifying information, medical history, employment, credit information, and relationships.[189] **Kaseware**, an investigation management platform, provides software to fusion centers to analyze SARs reports.[190]

As discussed further in Section IV, the fusion center funding ecosystem and reliance on corporate products was driven by industry-backed law enforcement associations, and in particular, the public-private revolving door of relationships in the National Fusion Center Association (NFCA). Many companies, especially the data brokers who provide their technology to fusion centers, also actively spend hundreds of thousands of dollars on lobbying around policies that regulate and build oversight for data sharing practices.[191]

The UASI to Fusion Center Funding Pipeline

Despite sharp Congressional criticism of fusion centers, UASI and HSGP grants continue to funnel DHS funding to fusion centers across the country.[192] As of 2021, federal funds could still provide up to a third of all fusion center budgets.[193] According to NFCA testimony to the Senate in 2021, **some fusion centers are nearly entirely grant-funded through UASI and/or SHSP**.[194]

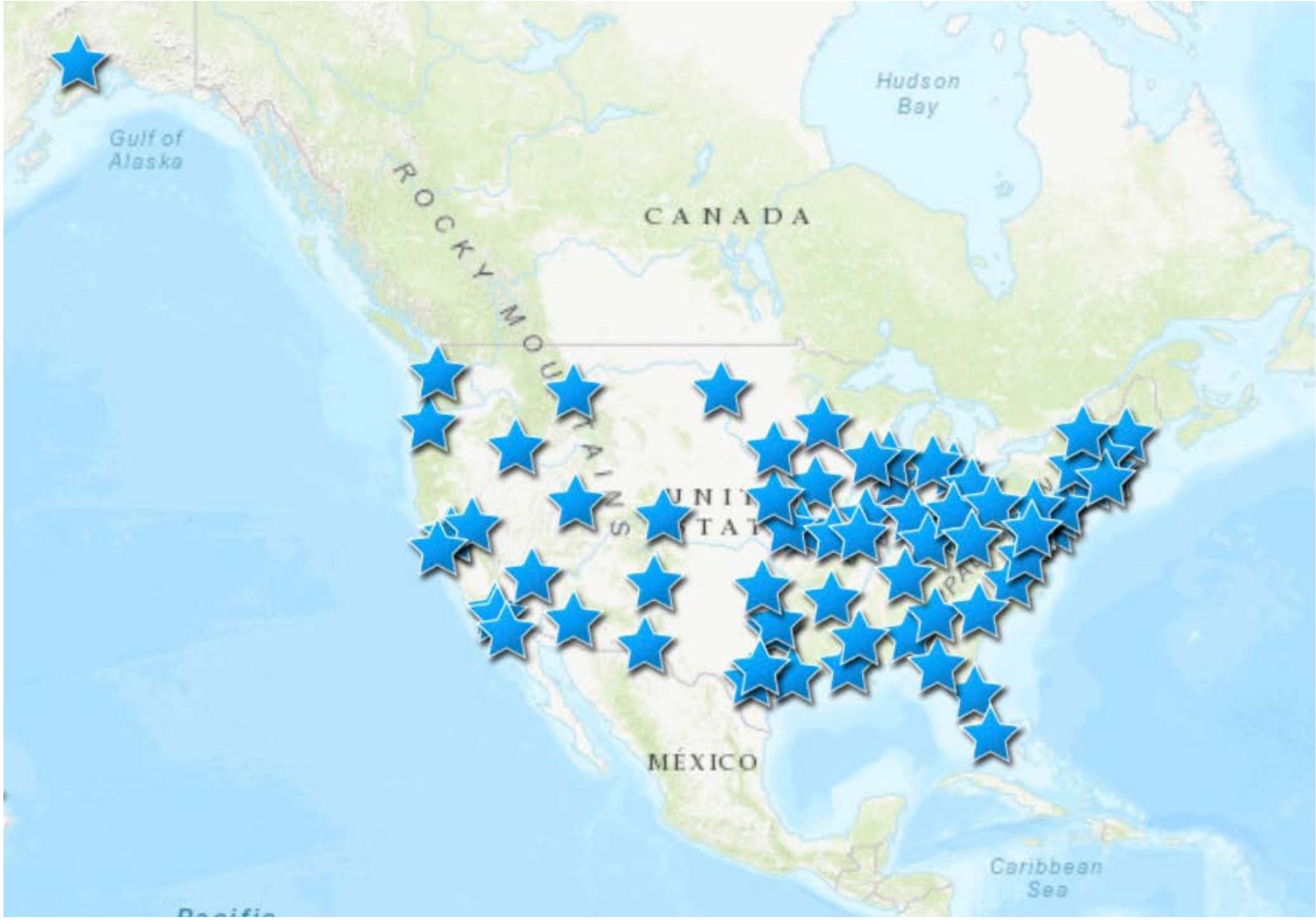
Our research confirms that UASI funding continues to boost the budgets of fusion centers in Boston, Illinois, and Los Angeles, amplifying their harm to our communities. We include examples below, but these numbers don't paint the full picture, as government agencies denied or did not reply to many of our records requests, likely obscuring additional funding.

Fusion center operations and information services: In Chicago, "Fusion Center" was one of nine budget categories in UASI grant documents. From 2018 to 2021, $9 million in Chicago UASI funds went directly to this fusion center category.[195] Boston's 2020 UASI funding request included $3.2 million linked to its fusion center (the Boston Regional Intelligence Center or BRIC), with $510,000 specifically earmarked for "hardware, software programs and data/ information technology services."[196] In Los Angeles, from 2018 to 2019, at least $11.8 million of UASI funding was allocated to its fusion center (the Joint Regional Intelligence Center or JRIC).[197] A 2019 contract extension shows that between 2016 and 2022, the LA County Sheriff's Department specifically budgeted almost $24 million in UASI funds for a contract with Palantir for JRIC.[198]

Intelligence analysts: UASI grants fund the salaries of fusion center staff. Boston's 2020 UASI funding includes $1.8 million for cybersecurity and intelligence analysts at its fusion center—the Boston Regional Intelligence Center (BRIC)—and another $308,500 for intelligence analysts specifically focused on "Countering Domestic Violence Extremism," programming that is likely similar to CVE, as described in Section II.[199] Between 2018 and 2021, the Illinois State Police requested $5.7 million of UASI funding for "Salary for Terrorism Analysis."[200] Between 2018 and 2019, about $11.3 million of Los Angeles's UASI funding for JRIC went to intelligence analyst salaries.[201]

Fusion Centers Are Key to the War on Terror

Fusion centers, with infrastructure built and policies maintained by corporations, are a key example of the public-private collaborations sustaining the localized War on Terror and its investments in mass surveillance, information sharing systems, and militarized policing. Funded by DHS counterterrorism grants, fusion centers have played a clear role since the early 2000s in the counterterrorism profit cycle—and the way this profit cycle obscures itself from public oversight. Section IV will expand on how corporations and law enforcement collaborate through industry-funded law enforcement associations and think tanks to sustain counterterrorism infrastructure like fusion centers.



Fusion center locations in the continental United States. Source: nfcausa.org.

IV. THROUGH LAW ENFORCEMENT ASSOCIATIONS, INDUSTRY & GOVERNMENT CO-DESIGN HOMELAND SECURITY POLICY

Law enforcement associations and the conferences they host play a major role in shaping homeland security policy today. One of the primary functions of law enforcement associations is to advocate for increased resources for their membership, which in recent years has meant more funding for surveillance and policing technology. Therefore, it is no surprise to see these organizations' sponsorship rosters include companies that produce and profit from the same surveillance and policing technology that these associations promote. **As financial backers and sponsors, corporations wield power over the associations' activities and gain a critical seat at the table.**

Tech and surveillance corporations enmesh themselves into law enforcement and homeland security associations in many ways: direct sponsorship of the organizations and conferences, exhibition at their gatherings to market their tools directly to law enforcement, behind-the-scenes relationship building with government officials, and securing executive board positions within these organizations. **This web of corporate involvement gives corporations opportunities to push for greater surveillance and tech "solutions" to public safety**.

Law enforcement associations have been convening annual national gatherings and year-round events that bring tech companies together with government officials.[202] Post-9/11, these associations grew to include fusion center leadership and DHS policymakers. With corporate influence, these associations set much of the agenda for public-private data sharing and surveillance practices across our communities. **These associations and gatherings serve as venues for growing alliances between homeland security personnel, law enforcement, and tech corporations**.

Homeland Security Law Enforcement Associations Today

Many of the law enforcement associations we profile here, from the early 2000s to today, are funded and sponsored by household brands like **AT&T** and **Motorola Solutions** as well as tech companies that own and profit from massive amounts of consumer data, like **Microsoft** and **Equifax**. Law enforcement associations bring government officials and larger tech companies into the same room with lesser-known data brokers, predictive analytics and artificial intelligence companies, and data surveillance companies. Through these associations, tech corporations fund and sustain the forums and conferences that promote the policing technology and data broker industries, which have now become the backbone of fusion centers and core recipients of DHS grant funding.

Law enforcement and industry organizations also function as an advocacy arm for a sprawling network of corporations that sustain fusion centers and provide surveillance technology to local and state agencies. In some cases, these same associations produce the industry-backed research and reports that get presented to legislatures and policymakers. The groups outlined below also bring tech executives into the same room with law enforcement leaders, homeland security policymakers, and government grantmakers and procurement officers, creating an ideal venue for corporate capture of the counterterrorism narrative and public safety policy world.

There are a vast number of both industry and law enforcement groups that advocate on behalf of the hundreds of surveillance corporations that provide technology for fusion centers and to local and state agencies in the name of counterterrorism. **In this section, we focus on four groups with significant ties to tech corporations through corporate sponsorship programs and board positions that shape homeland security policy today.**

What these four examples reveal is that **the corporations that stand to profit from homeland security not only have a seat at the table when it comes to creating policy and infrastructure, but are often the ones paying for the table to be there in the first place.**

National Fusion Center Association (NFCA)

The National Fusion Center Association (NFCA) is a corporate-backed lobbying organization that represents the interests of over 70 state and major urban area fusion centers across the United States.[203] One of their stated missions is to promote "ethical" information sharing between law enforcement agencies in the interest of public safety.[204] However, a 2012 bipartisan Senate report on fusion centers describes the NFCA as a private organization that "purports" to represent all fusion centers, but in reality "it is funded by corporations who seek to do business with fusion centers."[205]

The NFCA's core activity since its founding in 2009 has been to lobby the federal government to maintain and expand funding to fusion centers.[206] During the 2011 federal budget season when many federal agencies faced massive budget cuts, NFCA's Founding Executive Director Ross Ashley successfully argued for maintaining funding to fusion centers, saying "We can't afford, from an economic standpoint or any other standpoint, to be attacked," drawing an explicit connection between national security and economic stability.[207] Prior to founding the NFCA, Ashley served as a DHS grants administrator at FEMA and made similar pleas to Congress in 2011 to consider using more general UASI grants to support fusion centers as a way to stabilize their continued funding.[208]

While NFCA claims to be an independent voice supporting the best interests of fusion centers by educating the federal government on the issues they face, their extensive list of corporate tech sponsors tells a different story. Corporate sponsors include household technology names like **Microsoft, LexisNexis, Moonshot** (funded by **Google**),[209] and **Appriss** (owned by **Equifax**), police surveillance technology companies like **ShotSpotter**, **Clearview, Skopenow, Kaseware,** and **i2,** and smaller data broker and law enforcement surveillance firms that are vying for business from fusion centers.[210] Corporate sponsorship from well-known vendors in the tech and police surveillance industry suggests that these companies have much to gain and profit from NFCA's lobbying and advocating on behalf of fusion centers. Arguably, these tech and surveillance giants also lend credibility to NFCA and the entire enterprise of fusion centers.

Recently, in May 2022, the NFCA hosted a call with over 150 law enforcement officials nationwide, including members of the FBI and DHS, to discuss threats of violence and protests in the aftermath of the Supreme Court ruling that overturned Roe v. Wade.[211] In recent years, fusion centers have aided law enforcement in surveilling protesters across different movements and cities.[212] **Many of the same corporations that publicly claim to support racial, environmental, and reproductive justice are funding the policing and surveillance of protesters demonstrating for these causes.**

National Homeland Security Association (NHSA)

The National Homeland Security Association (NHSA) first began hosting their annual gatherings in 2005.[213] Their primary mission is to support the exchange of information among jurisdictions that receive UASI funding from the Department of Homeland Security.[214] Their annual conference, which has sold out for the past several years,[215] brings together emergency management, law enforcement, and homeland security professionals with heads of fusion centers from around the country.[216]

Corporations in the business of "security" that benefit from UASI funding are also in attendance at NHSA as both exhibitors and sponsors of the event. Corporate exhibitors and sponsors at the 2022 conference included cyber threat intelligence companies like **Flashpoint** (also a Tier 1 sponsor of the NFCA) and **Haystax**, which provides cloud capacity to fusion centers across the country, including in Boston and Los Angeles.[217] Other notable sponsorships include telecommunications giants like **Motorola Solutions** and **FirstNet (AT&T)**, as well as **D2iQ**, a software company based in San Francisco.[218]

FEMA
Christopher Logan
Acting Assistant Administrator
Federal Emergency Management Agency - Grant Programs
Live captioning available via the conference app
National Homeland Security Conference
2019
PHOENIX
National Homeland Security Conference 2019
#NHSC2019

Source: Twitter @NationalUASI.

Integrated Justice Information Systems (IJIS) Institute

The Integrated Justice Information Systems (IJIS) Institute is an industry offshoot of a 1999 Department of Justice (DOJ), Office of Justice Programs (OJP), and Bureau of Justice Assistance (BJA) project that brought together "members of the justice information technology community" with industry leaders.[219] In 2001, IJIS Institute registered as a non-profit organization and now hosts a Board of Directors stacked with tech executives from companies like **Microsoft**, **FirstNet (AT&T**), **IBM**, and **Thomson Reuters**.[220] They launched with 14 charter member corporations in 2001 and now have nearly 400, including "sustaining members" such as **Microsoft** and **FirstNet (AT&T)**.[221] Other notable corporate sponsors currently include: **NEC**, **Amazon Web Services,** a major government cloud services provider (including to fusion centers), **Axon,** which provides body cameras and drone technology to police, **IBM**, and **Motorola Solutions**.

IJIS's key initiatives focus primarily on law enforcement and security, including fusion center assistance and Suspicious Activity Reporting (SARs) programs. IJIS is also listed as a partner with various law enforcement associations and advocacy initiatives, including a partnership with the National Policing Institute (formerly the National Police Foundation).[222]

IJIS Institute produces industry-backed research and reports on topics related to information sharing, law enforcement, and fusion centers, including a 2019 report co-authored with the International Association of Chiefs of Police arguing in support of facial recognition technology.[223] They've co-authored manuals on fusion center data management best practices and serve as a go-to on issues related to data sharing, effectively operating as an industry think tank, shaping and defining new paths for private and public partnerships regarding surveillance.[224] **In 2021, IJIS itself received funding through a Bay Area UASI grant to the tune of $452,000 to provide trainings for law enforcement.[225]**

IJIS's leadership and board also provide a glimpse into the revolving door between tech and non-profit tech think tank advocacy groups. Glenn Archer, a former IJIS Executive Director and long-time board member is now the Vice President of Justice Intelligence at **Appriss**, a data analytics company owned by **Equifax** that has multiple contracts with law enforcement agencies and has notoriously contracted with ICE, allowing the agency to bypass sanctuary city policies.[226] Archer also served as the former Executive Director of the National Fusion Center Association.[227] Archer is a prime example of how data industry executives build relationships with policymakers, agenda setters, and grantmakers through affiliation within these key groups that organize the fusion center industry.

International Association of Chiefs of Police (IACP)

The International Association of Chiefs of Police (IACP) is a non-profit organization that refers to itself as the "world's largest and most influential professional association for police leaders" with membership in over 170 countries.[228] The organization sees itself as helping shape the future of policing through conducting research, hosting trainings and programming, as well as organizing an annual conference with heavy presence from technology companies.[229] IACP also hosts a technology-specific conference.[230]

Among their list of corporate sponsors are **Axon**, **FirstNet (AT&T)**, **Flock Safety** (which sells ALPR technology), **Motorola Solutions**, **Oracle**, and **T-Mobile**.[231] Additionally, they list partnership and grant relationships with **Microsoft**,[232] the **Motorola Foundation** and **Target Corporation,**[233] and other federal agencies.[234]

In 2002, IACP passed a resolution urging Congress to create the Department of Homeland Security,[235] as well as multiple resolutions supporting the continued funding of fusion centers in the years since.[236] IACP lists funding to support fusion centers and UASI funding as top policy priorities.[237]

IACP plays an important role in homeland security decision-making through its relationships with the federal government. Current IACP Executive Director and CEO Vincent Talucci serves on the Homeland Security Advisory Council (HSAC), which plays a role in determining priorities for DHS.[238] Prior to joining IACP, Talucci worked at the data firm **SAS**, a leading law enforcement software and predictive analytics company, where he served as Principal Advisor for Law Enforcement, State and Local Government Practice.[239]

Corporate Capture of Homeland Security

While these groups are just a small slice of a much larger network of organizations working to prop up the homeland security industry, they demonstrate how deeply corporate interests are embedded within these associations' mission and focus. While they attempt to appear as neutral experts on public safety and information sharing, their list of financial backers and board memberships reveal just how closely tied they are to the industries profiting from the homeland security project. These organizations and associations play a key role in legitimizing the interests of the sprawling network of corporations that sustain fusion centers and the power of the homeland security industry. Our analysis is that these associations and their corporate partners help to prop up the *real* aim of homeland security and counterterrorism projects, which is to grow profits for corporations through propping up an ever-expanding, xenophobic, and racist surveillance state that holds us all captive.

CONCLUSION

The War on Terror is built on the lie that surveillance, policing, and war make us safer. In reality, the War on Terror has devastated the lives of Muslim, Black, Brown, Asian, Indigenous, and immigrant communities across the world and in the United States. Twenty years after 9/11, DHS and its corporate partners continue to drive this violence to an unprecedented scale, relying on "emergency" and "counterterrorism" to expand the police state.

Our report reveals that "national security" and "counterterrorism" are masquerades for profit and militarized policing. DHS counterterrorism grants, especially the Urban Area Security Initiative (UASI), have steered billions towards mass surveillance infrastructure like fusion centers. Through lobbying, a revolving door, and sponsorship of law enforcement associations, corporations have helped create and expand demand for these technologies, virtually guaranteeing their own revenues.

DHS created a state of permanent emergency to justify rampant surveillance and embed its mission into local policing across the country. Corporations like **Microsoft, LexisNexis, ShotSpotter, Palantir,** and **Motorola Solutions** have increased their revenues by contributing to the normalization and expansion of this perpetual homela.

As the movement to divest from policing and invest in our communities becomes stronger and our demands to curb ever-expanding surveillance systems grow louder, we must also address and challenge the ways the homeland security state continues to harm our communities.

RECOMMENDATIONS

It's time to end the counterterrorism funding streams and policies that supercharge policing in our neighborhoods and make corporations richer. DHS and policing in our neighborhoods are inextricably connected, and as we work to divest from police and surveillance, we must divest also from homeland security. Dismantling the Department of Homeland Security and the public-private infrastructure that fuels it are essential steps to ensure our communities are safe from all threats of state violence.

These recommendations are not exhaustive, and we hope that they serve as a short list of starting points or opportunities to amplify existing campaign work. Our recommendations are rooted in a framework that envisions a world beyond surveillance and policing.

Local & State Action

1. **To promote true community safety, city and state officials should reject Urban Area Security Initiative funding and instead invest in public services like education, housing, and healthcare.**

   City and state officials can introduce budgeting resolutions to prohibit their cities and states from receiving specific types of grant funding from DHS, or vote against approval of purchases for surveillance and policing technology with awarded UASI funding. Instead of funding for surveillance and policing, city and state officials can invest in public services, prioritizing communities harmed by the counterterrorism cycle, and push the federal government to provide critical disaster response funding that is not tied to policing.

2. **To protect their residents, city and state officials should divest all funding from fusion centers and other surveillance networks in local and state budgets and instead invest those funds in public services.**

   Cities and states can divest funding from policing and surveillance networks, especially when they are established in the name of counterterrorism operations. As a process towards ending contracts for policing and surveillance technology, cities can institute accountability and oversight mechanisms on the technology being purchased, policies and reporting requirements on its use, and the impacts on communities. Municipalities and states can also invest in changes to local procurement processes, to limit contracts with vendors that profit from the extractive data economy and surveillance systems.

Federal Action

1. **Congress should immediately cut Homeland Security Grant Program (HSGP) funding by 50 percent and separate funding for emergency response and immigration services from the DHS budget, on the path to total divestment.[240]**

   The Department of Homeland Security's consistent budget increases have fueled the pipeline of local police militarization and mass surveillance infrastructure for two decades.[241] DHS's budget for HSGP can be cut by 50%, with a focus on reducing funding for law enforcement activities and surveillance technology. This is an immediate and concrete first step to limit the role DHS plays in intensifying policing in our neighborhoods. Emergency response services, including services provided by FEMA, as well as essential immigration services, can be separated from DHS and counterterrorism programs including HSGP, as they were before the department's founding. Instead, our tax dollars can be invested in education, healthcare, infrastructure, and other public goods that create true safety.

2. **Congress and federal agencies should limit and regulate corporate data sharing and ensure that homeland security and policing exceptions are no longer used as loopholes for corporations to profit from mass data collection.**

   There are few meaningful protections for people's data, especially when it is collected by corporations and policing agencies. Congress should pass comprehensive federal privacy legislation which prohibits law enforcement agencies from buying or acquiring data from companies including surveillance corporations. Federal agencies like the Federal Trade Commission (FTC) should use their rulemaking processes to impose prohibitions and limitations on commercial surveillance, data collection and sharing, and policing technology, without any exceptions for policing and homeland security which harm communities of color the most.

Corporate Action

1. **Mass data collection and surveillance should not be profitable, and companies should not be able to make them an essential part of their business model. Corporations like Microsoft, LexisNexis, and Motorola Solutions should not profit off mass consumer data collection, information sharing, and surveillance.**

   As a first step toward addressing how their products harm communities, corporations must terminate contracts with policing and surveillance agencies for these technologies. Corporations must stop selling technology like consumer databases, predictive policing software, license plate readers, facial recognition, and gunshot detection to serve the mission of racialized policing. Surveillance corporations and data brokers must end data sharing partnerships with law enforcement agencies.

2. **Corporations should withdraw funding and sponsorship from law enforcement associations and think tanks pushing counterterrorism policies that harm our communities. Corporations like Microsoft, LexisNexis, and Motorola Solutions shouldn't be driving policies that fuel policing in our communities and make a profit from these contracts.**

   Corporations fund and fuel associations and think tanks that bring together law enforcement officials, which often promote policies that drastically expand the police and surveillance state, and rely on these same companies' products. To uphold corporate statements in support of racial and social justice, corporations must divest financially from these associations and end their partnerships.

3. **Stakeholders of corporations like Microsoft, LexisNexis, and Motorola Solutions—including shareholders, workers, and consumers—can challenge the role these corporations play in exacerbating racist homeland security policy and sustaining the counterterrorism profit cycle.**

   Corporations rely on their shareholders, workers, and consumers. Shareholders can utilize tools such as shareholder resolutions at annual meetings to demand disclosures about corporate profiteering from police technology. Workers can organize to speak out about these partnerships.[242] Especially at consumer-facing and publicly-traded companies like **Microsoft** and **LexisNexis**, stakeholders can challenge corporate sales of technology to law enforcement and demand corporations be transparent and accountable for their operations with these agencies.[243] Students and faculty at universities can demand that their institutions divest from companies that uphold the counterterrorism profit cycle.[244]

APPENDIX A: UASI-FUNDED CORPORATIONS

UASI funds the acquisition of invasive surveillance and militarized policing technology at the state and local levels. This chart shows examples of prominent corporations that benefit from UASI funding and sell DHS-authorized equipment, highlighting some of the examples we found through our research. Many of these same corporations partner with industry-funded law enforcement associations to advocate for increased counterterrorism grant funding and market their products to law enforcement agencies at association conferences.

Company	UASI-Funded Violence
Microsoft	Microsoft built and maintains New York City's Domain Awareness System (DAS), the NYPD's real-time surveillance system. DAS increases the NYPD's ability to target and criminalize Black, Brown, and immigrant New Yorkers. Both Microsoft and the police profit when other cities buy the system. DAS is funded by at least $488.8 million in federal homeland security grants,[245] and at least at one point UASI funded the entire budget for DAS.[246]
Motorola Solutions	Motorola Solutions advertises its radio communications technology as eligible for UASI funding, expanding policing capabilities and budgets. In 2016, Chicago signed a five-year **$25 million** contract with **Motorola Solutions** paid for with UASI funds.[247] Between 2016 to 2020, the Los Angeles Police Department used over **$24 million** in UASI funds to upgrade its radio systems, likely contracts with Motorola Solutions.[248]
Vigilant Solutions	UASI funding pays for automatic license plate readers (ALPRs) and database access from **Vigilant Solutions** (now owned by Motorola Solutions), allowing police to track people's movements historically and in real time and share that data with federal agencies like ICE. Cities like Los Angeles and Boston use UASI funds to pay for ALPR technology.[249] From 2016 to 2020, Los Angeles spent at least **$1.27 million** on ALPRs, likely its contracts with Vigilant Solutions.[250]
ShotSpotter	Cities across the country rely on UASI funding for **ShotSpotter**'s controversial gunshot detection technology which has been criticized for inaccuracies that further police violence and targeting of communities of color.[251] Cities across the Boston region have used UASI funding to pay for ShotSpotter for almost a decade.[252] ShotSpotter advertises its technology as eligible for UASI funding.
Palantir	In Los Angeles, more than **$1.1 million** in UASI funding was used to pay for an "advanced data fusion" platform, licenses, and trainings, likely from **Palantir**, a data mining company that has patented "crime risk forecasting" and implements predictive policing.[253] The LA County Sheriff's Department also contracted with Palantir for the Joint Regional Intelligence Center (JRIC), budgeting almost **$24 million** for access to the platform.[254]
Dataminr	In New York City, **$500,000** in UASI funding was used to pay for **Dataminr**, a social media surveillance company. A Public Records Officer reported that the New York Office of Emergency Management, which holds this contract, shares it with the NYPD, highlighting how UASI ties emergency response funding to policing.[255]

ENDNOTES

[1] We use the phrase “War on Terror” throughout the report to refer to the wars abroad that targeted Muslim-majority regions as well as the domestic counterterrorism apparatus that was built by the federal government and corporations which criminalized, targeted, and killed Muslim, Black, Brown, Asian, and immigrant communities in the aftermath of 9/11. We put the term “War on Terror” in quotes throughout the executive summary to signify that we believe this project did not actually take on “terror,” and instead weaponized the frame of safety and security to harm our communities. So as not to distract the reader, we will not use quotation marks around this phrase throughout the rest of the report.

[2] Deepa Fernandes, “The Immigration-Industrial Complex: Booming Business At the Expense of Immigrants Rights?,” in Targeted: Homeland Security and the Business of Immigration (Seven Stories Press, 2011), 170.

[3] Similar to “War on Terror,” we use the phrases “counterterrorism,” “homeland security,” “national security,” and “emergency” throughout the report to describe the words used by the US and corporations to justify the War on Terror. We put them in quotes throughout the executive summary to signify that we do not think the policies described as such correspond to the definitions of the words used, and instead are often utilized to evoke fear and urgency. So as not to distract the reader, we will not use quotation marks around these phrases throughout the rest of the report.

[4] A majority of the companies discussed in this report are corporations. We use the term corporations throughout to represent the companies in this report, although a few may not be legally classified as corporations.

[5] “DHS Budget,” Department of Homeland Security, last accessed Oct. 25, 2022, https://www.dhs.gov/dhs-budget.

[6] Dan Verton, “DHS Had Little Choice But to Sign Microsoft Deal, Despite Security Flaws,” Computer World, July 21, 2003, https://www.computerworld.com/article/2571421/dhs-had-little-choice-but-to-sign-microsoft-deal--despite-security-flaws.html.

[7] For FY 2002–2015, our analysis uses data from a 2016 CRS Report: Shawn Reese, “Department of Homeland Security Preparedness Grants: A Summary & Issues,” CRS (2016): 16, https://www.everycrsreport.com/files/20161028_R44669_371198ad15aa9a4c4775413d98ff668c607a4b70.pdf. For FY 2016–2022, our analysis uses data from the FEMA information page on HSGP. “Homeland Security Grant Program,” Federal Emergency Management Authority, last accessed Nov. 17, 2022, https://www.fema.gov/grants/preparedness/homeland-security.

[8] UASI funding has been $615 million every year since 2020, increasing from $580 million annually beginning in 2016. “Homeland Security Grant Program,” FEMA.

[9] “Microsoft & Illinois State Police Collaborate on Best Practices and Information Technology Architecture for Homeland Security Fusion Centers,” Microsoft, Dec. 5, 2007, https://news.microsoft.com/2007/12/05/microsoft-and-illinois-state-police-collaborate-on-best-practices-and-information-technology-architecture-for-homeland-security-fusion-centers.

[10] “Fusion Centers in Illinois,” ACLU, last accessed Oct. 24, 2022, https://www.aclu-il.org/en/publications/fusion-centers-illinois.

[11] “Fusion Center Locations & Contact Information,” DHS, last accessed Oct. 24, 2022, https://www.dhs.gov/fusion-center-locations-and-contact-information.

[12] Mariame Kaba discusses defunding the New York Police Department (NYPD) to 50%. This is a step to making organizations like DHS obsolete and refunding basic community services. Mariame Kaba, “Yes, We Literally Mean Abolish the Police,” N.Y. Times, June 12, 2020, https://www.nytimes.com/2020/06/12/opinion/sunday/floyd-abolish-defund-police.html; This demand builds on calls in Just Futures Law’s Defunding the DragNet to reduce DHS’s budget for biometrics & surveillance networks by 50%. Dinesh McCoy, “Defunding the Dragnet,” Just Futures Law (2011): 8, https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/635c0a8119df2627cab1c567/1666976386334/JFL_Report-DefendingTheDragnet_111521.pdf.

[13] Fernandes, “The Immigration-Industrial Complex,” 169–71.

[14] Harsha Walia, “Historic Entanglements of US Border Formation,” in Border & Rule: Global Migration, Capitalism & the Rise of Racist Nationalism (Chicago: Haymarket Books, 2021), 33–37.

[15] “DHS Budget,” Department of Homeland Security.

[16] “The Cost of Immigration Enforcement and Border Security,” American Immigration Council, Jan. 20, 2021, https://www.americanimmigrationcouncil.org/research/the-cost-of-immigration-enforcement-and-border-security.

[17] “A History of the Drug War,” Drug Policy Alliance, last accessed Oct. 27, 2022, https://drugpolicy.org/issues/brief-history-drug-war.

[18] Mohita Anand & Constantin Schreiber, “The NSEERS Effect: A Decade of Racial Profiling, Fear & Secrecy,” Penn State Law Rights Working Group (2012): 4 & 9, https://pennstatelaw.psu.edu/_file/clinics/NSEERS_report.pdf. “Fact Sheet: Changes to National Security Entry/Exit Registration System (NSEERS),” DHS (2003): 4, http://www2.gtlaw.com/practices/immigration/news/2003/12/01a.pdf.

[19] Andrew Selsky, “New Report Shows DHS Gathered Intel on Portland Black Lives Matter Protestors,” PBS, Oct. 28, 2022, https://www.pbs.org/newshour/nation/new-report-shows-department-of-homeland-Security-gathered-intel-on-portland-black-lives-matter-

protestors; Alleen Brown & Sam Richards, "Low-Flying DHS Helicopter Showers Anti-Pipeline Protests With Debris," June 8, 2021, Intercept, https://theintercept.com/2021/06/08/line-3-pipeline-helicopter-dhs-protest.

[20] Fernandes, "The Immigration-Industrial Complex," 173.

[21] Brendan Koerner, "The Security Traders," Mother Jones, Sept. 2002, https://www.motherjones.com/politics/2002/09/security-traders.

[22] "Homeland Security Grant Program," FEMA; Allison McCartney, Paul Murray, & Mira Rojanasakul, "After Pouring Billions Into Militarization of US. Cops, Congress Weighs Limits," Bloomberg, July 1, 2020, https://www.bloomberg.com/graphics/2020-police-military-equipment; Ali Watkins, "How the N.Y.P.D. Is Using Post-9/11 Tools on Everyday New Yorkers," N.Y. Times, Oct. 13, 2021, https://www.nytimes.com/2021/09/08/nyregion/nypd-9-11-police-surveillance.html.

[23] See note 7 for calculation on $28 billion of HSGP funding from 2002 to 2022.

[24] BigTechSellsWar.com, ACRE, LittleSis, & MPower Change, last accessed Oct. 24, 2002, https://bigtechsellswar.com.

[25] Jasson Perez, Alyxandra Goodwin, & Jessica Quiason, "21st Century Policing: The Rise & Reach of Surveillance Technology," ACRE (2021): https://acrecampaigns.org/wp-content/uploads/2021/03/acre-21stcenturypolicing-r4-web.pdf.

[26] Peter Swire is a law professor who was a former advisor to President Clinton on technology and privacy issues. In the post-9/11 period, he commented about his fears that the private sector would capitalize on the "homeland security" fervor in a moment of economic turmoil to evade constitutional protections and undermine civil liberties. Koerner, "The Security Traders."

[27] Russ Mitchell, "Business; Recovery in Technology Spending Is Still Elusive," N.Y. Times, June 23, 2002, https://www.nytimes.com/2002/06/23/business/business-recovery-in-technology-spending-is-still-elusive.html; David Marguluis, "Managers Survey: Tech Spending Priorities for 2002," ZDNet, Jan. 9, 2002, https://www.zdnet.com/article/managers-survey-tech-spending-priorities-for-2002.

[28] Alorie Gilbert, "IT: New Profits in Old Glory?," ZDNet, July 12, 2022, https://www.zdnet.com/article/it-new-profits-in-old-glory-5000124027.

[29] Gilbert, "IT: New Profits in Old Glory?"

[30] BigTechSellsWar.com, ACRE, LittleSis, & MPower Change.

[31] Koerner, "The Security Traders."

[32] Koerner, "The Security Traders."

[33] "President's Homeland Security Advisory Council," CNN, June 12, 2002, http://www.cnn.com/2002/ALLPOLITICS/06/12/security.council.members/index.html; "Homeland Security Council," George W. Bush White House Archives, last accessed Oct. 24, 2022, https://georgewbush-whitehouse.archives.gov/hsc.

[34] Fernandes, "The Immigration-Industrial Complex," 171–75.

[35] "Department of Homeland Security," IACP, Nov. 1, 2022, https://www.theiacp.org/resources/resolution/department-of-homeland-security.

[36] 107th Congress, "Homeland Security Act of 2002: Section 508," Department of Homeland Security (2002): 81, https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf.

[37] "Homeland Security Act of 2002: Section 509."

[38] Gilbert, "IT: New Profits in Old Glory?"

[39] Gilbert, "IT: New Profits in Old Glory?"

[40] Philip Shenon, "Aftereffects: Domestic Security," N.Y. Times, Apr. 4, 2003, https://www.nytimes.com/2003/04/29/us/aftereffects-domestic-security-former-domestic-Security-aides-make-quick-switch.html. For more information, see Jay Stanley, "The Surveillance-Industrial Complex: How The American Government in Conscripting Businesses and Individuals in the Construction of a Surveillance Society." ACLU (2004): 28, https://www.aclu.org/sites/default/files/FilesPDFs/surveillance_report.pdf.

[41] "Thomas J. Ridge, Secretary of Homeland Security 2003-2005," DHS, last accessed Nov. 17, 2022, https://www.dhs.gov/thomas-j-ridge.

[42] "Tech-Savvy Gov.: Bush's Mate?," Wired, May 31, 2000, https://www.wired.com/2000/05/tech-savvy-gov-bushs-mate.

[43] Verton, "DHS Had Little Choice But to Sign Microsoft Deal, Despite Security Flaws."

[44] "The Spectrum Needs of Our Nation's First Responders," Hearing Before the Subcommittee on Telecommunications & the Internet, June 11, 2003, https://www.govinfo.gov/content/pkg/CHRG-108hhrg88424/html/CHRG-108hhrg88424.htm.

[45] "Client Profile: Motorola Inc," OpenSecrets, last accessed Oct. 24, 2022, https://www.opensecrets.org/federal-lobbying/clients/issues?cycle=2003&id=D000000355&spec=BUD&specific_issue=Fed+Budget+%26+Appropriations#specific_issue.

[46] "Motorola Solutions Annual Report 2003," Motorola, Inc. (2003): 11, https://stocklight.com/stocks/us/manufacturing/nyse-msi/motorola-solutions/annual-reports/nyse-msi-2003-10K-03621641.pdf.

[47] "Presumption of Guilt: Human Rights Abuses of Post-September 11 Detainees," Human Rights Watch (2002): 16 n.27, https://www.academia.edu/es/12299530/Presumption_of_Guilt_Human_Rights_Abuses_of_Post_September_11_Detainees_A_Human_Rights_Watch_report_%2016.

[48] William Matthews, "In the System," FCW, Jan. 20, 2002, https://fcw.com/workforce/2002/01/in-the-system/200746.

49 Today, LexisNexis Risk Solutions advertises SmartLinx as a records database that provides "instant" reports on individuals, including their personal connections, "neighboring households," businesses, assets, and "civil/criminal matters." SmartLinx is one of many LexisNexis products that buy, repackage, analyze, and sell intimate personal data on hundreds of millions of people to law enforcement."SmartLinx Person Report," LexisNexis Risk Solutions, last accessed Nov. 1, 2022, https://risk.lexisnexis.com/products/smartlinx-person-report.

50 Matthews, "In the System."

51 Associated Press, "Saudi Cleared of Sept. 11 Role, but Gets 4 Months for Visa Fraud," N.Y. Times, Jan. 5, 2002, https://www.nytimes.com/2002/01/05/national/saudi-cleared-of-sept-11-role-but-gets-4-months-for-visa-fraud.html.

52 Matthews, "In the System."

53 Identity fraud is commonly used as a reason to justify vastly increased data collection and data sharing, often for "identity verification" or authentication.

54 Gary Gordon & Norman Wilcox, "Identity Fraud: A Critical National and Global Threat," Economic Crime Institute (2003), http://www.lexisnexis.com/presscenter/hottopics/ECIReportFINAL.pdf.

55 "Industries," LexisNexis Special Services, last accessed Oct. 24, 2022, https://www.lexisnexisspecialservices.com/who-we-are/industries.

56 Fernandes, "The Immigration-Industrial Complex," 175–77.

57 Fernandes, "The Immigration-Industrial Complex," 175–77.

58 "Who's Behind ICE? The Tech & Data Companies Fueling Deportations," Mijente, National Immigration Project, Immigrant Defense Project (2018): https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf.

59 Robert O'Harrow Jr., "Introduction," in No Place to Hide (New York: Free Press, 2005), 1–3.

60 O'Harrow Jr., "Introduction," 1–3.

61 "Microsoft Hires National Security Honcho," CNET, Nov. 13, 2002, https://www.cnet.com/tech/tech-industry/microsoft-hires-national-security-honcho.

62 "We the People: Homeland Security from the Citizens' Perspective," The Council for Excellence in Government (2004): 2, https://share.ansi.org/Shared%20Documents/Standards%20Activities/Homeland%20Security%20Standards%20Panel/Emergency%20Communications%20and%20Citizen%20Readiness%20Joint%20Workshop/Workshop%20Meeting%20_1%20(December%202004)/Citizen%20Readiness%20Resources/CFEIG%20FINAL_VERSION_PDF.pdf.

63 "IT Leadership in a Security-Focused World," CSIS, last accessed Oct. 24, 2022, https://www.csis.org/events/it-leadership-security-focused-world.

64 "Microsoft Hires National Security Honcho," CNET.

65 "President's Critical Infrastructure Protection Board," Federal Register, last accessed Nov. 17 2022, https://www.federalregister.gov/agencies/president-s-critical-infrastructure-protection-board; "Microsoft Hires National Security Honcho," CNET.

66 "A Notice by the President's Critical Infrastructure Protection Board," Federal Register, Oct. 11, 2002, https://www.federalregister.gov/documents/2002/10/17/02-26456/october-11-2002.

67 Eric Geller, "Capitol Hill Angry Over Microsoft's Security Upcharge," Politico, Mar. 15, 2021, https://www.politico.com/newsletters/weekly-cybersecurity/2021/03/15/capitol-hill-angry-over-microsofts-security-upcharge-793983.

68 Susan Menke, "Byrne Leaves DHS for Microsoft," GCN, Nov. 19, 2003, https://gcn.com/2003/11/byrne-leaves-dhs-for-microsoft/295951.

69 Susan Menke, "Byrne Leaves DHS for Microsoft."

70 "BigTechSellsWar.com: Contract Calculator," ACRE, LittleSis, & MPower Change, https://bigtechsellswar.com/calculator; Michael Kwet, "The Microsoft Police State: Mass Surveillance, Facial Recognition, & the Azure Cloud," Intercept, July 14, 2020, https://theintercept.com/2020/07/14/microsoft-police-state-mass-surveillance-facial-recognition.

71 Kwet, "The Microsoft Police State."

72 "The LexisNexis Timeline," LexisNexis (2003): 1, https://www.lexisnexis.com/anniversary/30th_timeline_fulltxt.pdf

73 A data broker is a company that collects, repackages, and sells vast amounts of consumer data, in this case to government agencies including police and ICE.

74 "Federal Supply Service Authorized Federal Supply Schedule Pricelist," LexisNexis Special Services: 3, https://www.gsaadvantage.gov/ref_text/GS00F178DA/0VS1WS.3RIEVJ_GS-00F-178DA_LNSSIOLMGSA520561450OCT2020.PDF.

75 "Federal Supply Service," 3.

76 "Federal Supply Service," 3.

77 "Board of Directors," LexisNexis Special Services, last accessed Oct. 24, 2022, https://www.lexisnexisspecialservices.com/who-we-are/board-of-directors-3.

78 "MATRIX: Myths and Reality," ACLU, last accessed Oct. 24, 2022, https://www.aclu.org/other/matrix-myths-and-reality; Robert O'Harrow Jr., "Anti-Terror Database Got Show At White House," Wash. Post, May 21, 2004, https://www.washingtonpost.com/archive/politics/2004/05/21/anti-terror-database-got-show-at-white-house/9499a352-aad1-4157-917b-c8e03221ad66. Robert O'Harrow Jr., "LexisNexis To Buy Seisint For $775 Million," Wash. Post, July 15, 2004, https://www.washingtonpost.com/archive/business/2004/07/15/lexisnexis-to-buy-seisint-for-775-million/6c876089-ddb9-4d30-a8d4-4aacb742de67.

79 "LexisNexis Transformation Accelerates with Integration of ChoicePoint," LexisNexis, Oct. 15, 2008, https://www.lexisnexis.com/community/pressroom/b/news/posts/lexisnexis-transformation-accelerates-with-integration-of-choicepoint.

80 Sam Biddle, "ICE Searched LexisNexis Database Over 1 Million Times in Just Seven Months," Intercept, June 9, 2022, https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances.

81 "Who's Behind ICE?, 54–57.

82 Sam Biddle, "LexisNexis to Provide Giant Database of Personal Information to ICE," Intercept, Apr. 2, 2021, https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis; "'No Tech for ICE': Data Broker LexisNexis Sued for Helping ICE Target Immigrant Communities," Democracy Now, Aug. 19, 2022, https://www.democracynow.org/2022/8/19/immigrant_rights_groups_sue_data_broker.

83 Alfred Ng & Maddy Varner, "The Little-Known Data Broker Industry Is Spending Big Bucks Lobbying Congress," Markup, Apr. 1, 2021, https://themarkup.org/privacy/2021/04/01/the-little-known-data-broker-industry-is-spending-big-bucks-lobbying-congress."

84 "Who's Behind ICE?," 56.

85 Koerner, "The Security Traders."; "Firms Eye Anti-Terror Profiling," Wash. Times, Apr. 4, 2002, https://www.washingtontimes.com/news/2002/apr/4/20020404-041719-3080r.

86 Koerner, "The Security Traders."

87 "Privacy Office: Report to Congress," DHS (2004): 52, https://www.dhs.gov/xlibrary/assets/privacy/privacy_annualrpt_2004.pdf; Fred Cate, "Information Security Breaches and the Threat to Consumers," Articles by Maurer Faculty (2005): https://www.repository.law.indiana.edu/facpub/1291.

88 Joseph Menn, "Data Brokers Press for US Law," L.A. Times, Dec. 26, 2005, https://www.latimes.com/archives/la-xpm-2005-dec-26-fi-idlobby26-story.html.

89 "Microsoft Corporation: 2001 Lobbying Report," Senate.gov (2002): 3, https://lda.senate.gov/filings/public/filing/70402fd1-5c29-4997-b8f6-af14a5a4c5bc/print.

90 "Form S-1: Verint Systems," (2002): 34, https://verintsystems.gcs-web.com/node/8031/html.

91 "Biometric Identifiers & the Modern Face of Terror: New Technologies in the Global War On Terrorism," Hearing Before the Subcommittee on Technology, Terrorism, & Government Information (2001): https://www.govinfo.gov/content/pkg/CHRG-107shrg81678/html/CHRG-107shrg81678.htm.

92 Reese, "Department of Homeland Security Preparedness Grants: A Summary & Issues," 17.

93 "Homeland Security Grant Program," FEMA.

94 "Section 603: Homeland Security Grant Program," GovInfo, last accessed Oct. 28, 2022, https://www.govinfo.gov/content/pkg/USCODE-2016-title6/pdf/USCODE-2016-title6-chap1-subchapXV-partA-sec603.pdf.

95 See note 7 for calculation on $28 billion of HSGP funding from 2002 to 2022.

96 "Homeland Security Grant Program," FEMA.

97 Keith Bea, "Proposed Transfer of FEMA to the Department of Homeland Security," CRS (2002): https://www.everycrsreport.com/reports/RL31510.html.

98 "Homeland Security Grant Program," FEMA.

99 Jack Kern, "Report on the Fiscal 2023 Preliminary Plan and the Fiscal 2022 Mayor's Management Report for the New York City Emergency Management," NYC Council (2002): 4–5, https://council.nyc.gov/budget/wp-content/uploads/sites/54/2022/03/NYCEM.pdf.

100 "Targeted Violence and Terrorism Prevention Grant Program," DHS, last accessed Oct. 25, 2022, https://www.dhs.gov/tvtpgrants.

101 "What is CVE?," Muslim Justice League, last accessed Oct. 28, 2022, https://muslimjusticeleague.org/cve.

102 "#StopCVE Resources," StopCVE, last accessed Oct. 25, 2002, https://www.stopcve.com/about-us.html.

103 "What is CVE?," Muslim Justice League.

104 "Homeland Security Grant Program," FEMA.

105 "Fiscal Year 2022 Preparedness Grant Programs Final Allocation Announcement," FEMA (2022): 6, https://www.fema.gov/sites/default/files/documents/fema_information-bulletin-476-fy222-award-announcement-gpd.pdf.

106 "State Administrative Agency (SAA) Contacts," FEMA, last accessed Oct. 25, 2022, https://www.fema.gov/grants/preparedness/about/state-administrative-agency-contacts.

107 "DHS Announces $1.6 Billion in Preparedness Grants," DHS, May 13, 2022, https://www.dhs.gov/news/2022/05/13/dhs-announces-16-billion-preparedness-grants.

108 "DHS Announces $1.6 Billion in Preparedness Grants," DHS.

109 "Authorized Equipment List," FEMA, last accessed Oct. 25, 2022, https://www.fema.gov/grants/tools/authorized-equipment-list.

110 "Email from FOIL Officer at OEM," obtained by records request, Oct. 3, 2022, https://drive.google.com/file/d/1KTIRmBOEW9qMEyWQnfMEbLuLhgMLGhHB/view?usp=sharing.

111 Authorized Equipment List," FEMA.

112 Communications interoperability is defined by DHS as "the ability of anyone to talk with whomever they need to, whenever they need to, when properly authorized." This item approves various forms of communication technology that connect law enforcement agencies to one another. "Authorized Equipment List," FEMA.

113 Thomas Cincotta, "Manufacturing the Muslim Menace,"

Political Research Associates (2011): 18, https://www.cairflorida.org/images/pdf/Muslim_Menace_Complete.pdf.

114 Cincotta, "Manufacturing the Muslim Menace," 18. SSI rejected these claims.

115 "Get the BRIC Out of Boston," Muslim Justice League, last accessed Oct. 25, 2022, https://muslimjusticeleague.org/our-work/get-the-bric-out-of-boston.

116 "Shut Down the Spy Centers," Stop LAPD Spying, Apr. 12, 2014, https://stoplapdspying.org/shut-down-the-spy-centers.

117 "Stop Urban Shield Coalition Victory," War Resisters League, last accessed Oct. 25, 2022, https://www.warresisters.org/stop-urban-shield-coalition-victory-wrl-statement; Peter Hegarty, "Alameda County Loses Federal Money for Urban Shield," East Bay Times, Mar. 15, 2019, https://www.eastbaytimes.com/2019/03/15/alameda-county-loses-federal-money-for-urban-shield.

118 "Best Practices On How to Secure Federal or State Funding for ShotSpotter," ShotSpotter, May 4, 2016, https://www.shotspotter.com/system/content-uploads/FundingWebinar_May4_FINAL_050416_FINALDAYOFPRESENTATION.pdf; "FY22 Urban Areas Security Initiative Executive Summary," Motorola Solutions, last accessed Oct. 25, 2022, https://bit.ly/3N5PxQP.

119 "PoliceGrantsHelp.com Partners," Police Grants Help, last accessed Oct. 27, 2022, https://www.policegrantshelp.com/grant-sponsors.

120 "Specific Issues Reports for H.R.2471 by: Motorola Solutions, 117th Congress," OpenSecrets, last accessed Oct. 25, 2022, https://www.opensecrets.org/federal-lobbying/bills/specific_issues?id=hr2471-117&client_id=D000000355&cycle=2022.

121 "Specific Issues Reports for H.R.2471 by: Microsoft Corp, 117th Congress," OpenSecrets, last accessed Oct. 25, 2022, https://www.opensecrets.org/federal-lobbying/bills/specific_issues?id=hr2471-117&client_id=D000000115&cycle=2022.

122 "About NHSA," National Homeland Security Association, last accessed Oct. 25, 2022, https://www.nationalhomelandsecurity.org/about-nhsa.

123 "Mayor de Blasio Testifies Against Cuts to Vital Anti-Terror Funding," NYC.gov, Mar. 15, 2016, https://www1.nyc.gov/office-of-the-mayor/news/256-16/mayor-de-blasio-testifies-against-cuts-vital-anti-terror-funding#/0.

124 Nick Schwellenbach, "When Agencies Misuse FOIA's Law Enforcement Exemption," POGO, Mar. 15, 2021, https://www.pogo.org/analysis/2021/03/when-agencies-misuse-foias-law-enforcement-exemption.

125 "FY 2020 HSGP Investment Justification: Boston Urban Area," DHS (2020): 11, https://drive.google.com/file/d/1ztO13p0Abi9XOyZYYfeLI_cex3K_a87J/view?usp=sharing; Vivekae Kim, "Eyes & Ears in Cambridge," Harvard Crimson, Oct. 10, 2019, https://www.thecrimson.com/article/2019/10/10/shot-spotter.

126 "Best Practices On How to Secure Federal or State Funding for ShotSpotter," ShotSpotter, 19–20; Tracy Rosenberg, "Bay Area UASI 2020," Oakland Privacy, Mar. 9, 2020, https://oaklandprivacy.org/bay-area-uasi-2020.

127 Andy Grimm, "Activists Call for City to End Contract with ShotSpotter," Chicago Sun Times, July 29, 2021, https://chicago.suntimes.com/2021/7/29/22600484/activists-city-end-contract-shotspotter.

128 "FY16-20 LAPD UASI Funding."

129 "Cook County UASI Vendor Quotes," obtained by records request, https://drive.google.com/drive/folders/1PrU_pCKDV5xh9FyZi5R7issLKSUQf6PK?usp=sharing.

130 "FY 2020 HSGP Investment Justification: Boston Urban Area," DHS, 34.

131 "Editorial: Unblock California Police Radio Communications," Mercury News, Aug. 10, 2022, https://www.mercurynews.com/2022/08/10/editorial-unblock-california-police-radio-communications.

132 Historically, UASI funding has been used to pay for upgrades to LAPD's access to Motorola Solutions' radio systems as well. "Public Safety Committee Report," L.A. City, last accessed Oct. 25, 2022, https://cityclerk.lacity.org/councilagenda/CoverSheet.aspx-?ItemID=13088&MeetingID=581; "FY16-20 LAPD UASI Funding," https://drive.google.com/drive/folders/1bvx-rYDdU0Qm2V7lIcMEp0pmwuhSHZ8g7?usp=sharing.

133 This contract was signed by Chicago first and then Cook County used the model contract to incorporate itself into the order for Motorola Solutions' technology. "Professional Services Agreement: Contract No. 1650-15538," Cook County, June 8, 2016, https://opendocs.cookcountyil.gov/procurement/contracts/1650-15538.pdf, 23.

134 "Cook County UASI Vendor Quotes."

135 "FY 2020 HSGP Investment Justification: Boston Urban Area," DHS, 31.

136 "FY16-20 LAPD UASI Funding."

137 Caroline Haskins, "Scars, Tattoos, & License Plates: This Is What Palantir & The LAPD Know About You," Buzzfeed, Sept. 29, 2020, https://www.buzzfeednews.com/article/carolinehaskins1/training-documents-palantir-lapd.

138 "Palantir Played Key Role In Arresting Families for Deportation, Document Shows," Mijente, May 2, 2019, https://mijente.net/2019/05/palantir-arresting-families.

139 "FY16-20 LAPD UASI Funding."

140 "NYC OEM UASI Vendor List," obtained by records request, https://docs.google.com/spreadsheets/d/1VlTKs8VSYF2oGWjThZ5V_TrhSeL35kY_/edit?usp=shar-

ing&ouid=104848290978475337247&rtpof=true&s-d=true.

141 Sam Biddle, "Police Surveilled George Floyd Protests With Help from Twitter-Affiliated Startup Dataminr," Intercept, July 9, 2020, https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests. Sam Biddle, "Twitter Surveillance Startup Targets Communities of Color for Police," Intercept, Oct. 21, 2020, https://theintercept.com/2020/10/21/dataminr-twitter-surveillance-racial-profiling.

142 "Cell-Site Simulators/IMSI Catchers," Electronic Frontier Foundation, last accessed Nov. 1, 2022, https://www.eff.org/pages/cell-site-simulatorsimsi-catchers.

143 "FY16-20 LAPD UASI Funding."

144 Mike Katz-Lacabe, "Stingray Secrecy and the San Jose Police Department," Oakland Privacy, Mar. 2, 2022, https://oaklandprivacy.org/stingray-secrecy-and-the-san-jose-police-department; Mike Katz-Lacabe, "Anaheim Police Buy a $755,000 Nyxcell Cell Site Simulator," Center for Human Rights & Privacy, last accessed Nov. 1, 2022, https://www.cehrp.org/anaheim-police-buy-a-755000-nyxcell-cell-site-simulator; Darwin Bond Graham & Ali Winston, "Alameda County DA Seeks Controversial Surveillance Device," East Bay Express, July 1, 2015, https://eastbayexpress.com/alameda-county-da-seeks-controversial-surveillance-device-2-1.

145 Gang databases are an example of targeted surveillance, criminalizing mostly Black and Latinx men. The NYPD's gang database information is accessible through DAS. Alice Speri, "NYPD Gang Database Can Turn Unsuspecting New Yorkers Into Instant Felons," Intercept, Dec. 5, 2018, https://theintercept.com/2018/12/05/nypd-gang-database.

146 "Preparedness Grant Effectiveness Case Study: New York City," National Preparedness Assessment Division (2021): 8–9, https://www.fema.gov/sites/default/files/documents/fema_nyc-case-study_2019.pdf.

147 116th Congress, "Understanding the Importance of DHS Preparedness Grants," Congress.gov, Jan. 9, 2020, https://www.congress.gov/event/116th-congress/house-event/LC65234/text?s=1&r=2.

148 "FY 2020 HSGP Investment Justification: Boston Urban Area," DHS, 11.

149 Neal Ungerleider, "NYPD, Microsoft Launch All-Seeing 'Domain Awareness System' With Real-Time CCTV, License Plate Monitoring, Fast Company, Aug. 8, 2012, https://www.fastcompany.com/3000272/nypd-microsoft-launch-all-seeing-domain-awareness-system-real-time-cctv-license-plate-monito.

150 "Preparedness Grant Effectiveness Case Study: New York City," NPAD.

151 "Mayor de Blasio Testifies Against Cuts to Vital Anti-Terror Funding"; In Fiscal Year 2022, total funding for DAS was reported as $56 million for fiscal year 2022. Nevin Singh, "Report to the Committee on Finance and the Committee on Public Safety on the Fiscal 2023 Executive Plan," NYC Council Finance Division (2022): 7, https://legistar.council.nyc.gov/View.ashx?M=F&ID=10880378&GUID=B03E693E-2DEA-4B3C-BBDF-5570F5F96B21.

152 "New York City Police Department and Microsoft Partner to Bring Real-Time Crime Prevention and Counterterrorism Technology Solution to Global Law Enforcement Agencies," Microsoft, Aug. 8, 2012, https://news.microsoft.com/2012/08/08/new-york-city-police-department-and-microsoft-partner-to-bring-real-time-crime-prevention-and-counterterrorism-technology-solution-to-global-law-enforcement-agencies.

153 Malcolm Smith, "State Senate Democrats Alert Members Of Congress About New York's Homeland Security Needs," N.Y. Senate, Oct. 16, 2007, https://www.nysenate.gov/newsroom/press-releases/malcolm-smith/state-senate-democrats-alert-members-congress-about-new-yorks; "Mayor de Blasio Testifies Against Cuts to Vital Anti-Terror Funding," NYC.gov.

154 "Comments on the NYPD Jan. 11, 2021 Draft Impact & Use Policies, Pursuant to the Public Oversight of Surveillance Technology (POST) Act," Legal Aid Society (2021): 19–21, https://bit.ly/3sYxEKt; Jonathan Vanian, "Civil Rights Groups Urge Microsoft to End NYPD Partnership," Fortune, June 30, 2020, https://fortune.com/2020/06/30/civil-rights-groups-urge-microsoft-to-end-nypd-partnership; Kwet, "The Microsoft Police State: Mass Surveillance, Facial Recognition, & the Azure Cloud."

155 "FY16-20 LAPD UASI Funding."

156 "Palantir," Leadership in Counter Terrorism Alumni Association, last accessed Nov. 1, 2022, https://www.linct-aa.org/corporate-partners-articles-and-links/palantir.

157 "FY16-20 LAPD UASI Funding."

158 "FY 2020 HSGP Investment Justification: Boston Urban Area," DHS, 6 & 63.

159 "Chicago Budget Spreadsheet," obtained through records requests, https://drive.google.com/drive/folders/1GKNrjxRWPpzk97_PUhlI-V9R1ZyIkYNC?usp=sharing.

160 "Preparedness Grant Effectiveness Case Study: Chicago," FEMA (2020): 3, https://www.fema.gov/sites/default/files/documents/fema_chicago-covid-19-case-study_2020.pdf.

161 "NYC OEM UASI Vendor List"; "FY 2020 HSGP Investment Justification: Boston Urban Area," DHS, 67.

162 "NYC OEM UASI Vendor List."

163 "Email from FOIL Officer at OEM."

164 "FY16-20 LAPD UASI Funding"; "FY 2020 HSGP Investment Justification: Boston Urban Area," DHS, 9 & 44; "Cook County UASI Vendor Quotes."

165 "Written Testimony of FEMA Assistant Administrator for Grant Programs Brian Kamoie for a Senate Committee on Homeland Security and Governmental Affairs," DHS, Sept. 9, 2014, https://www.dhs.gov/news/2014/09/09/

written-testimony-fema-senate-committee-homeland-security-and-governmental-affairs.

166 Philip McHarris, Why Does the Minneapolis Police Department Look Like a Military Unit?, Wash. Post, May 28, 2020, https://www.washingtonpost.com/outlook/2020/05/28/explaining-militarized-police-response-protesters-after-killing-george-floyd; Andrew Lehren et. al, "Floyd Protests Renew Debate About Police Use of Armored Vehicles, Other Military Gear," NBC, June 20, 2020, https://www.nbcnews.com/news/us-news/floyd-protests-renew-debate-about-police-use-armored-vehicles-other-n1231288; Betsy Woodruff Swan, "Law Enforcement Officials Brace for Potential Violence Around SCOTUS Draft Opinion," Politico, https://www.politico.com/news/2022/05/05/law-enforcement-violence-scotus-draft-roe-opinion-00030509.

167 "Remarks by Homeland Security Secretary Janet Napolitano to the National Fusion Center Conference in Kansas City, Mo. on March 11, 2009," DHS, Mar. 13, 2009, https://www.dhs.gov/news/2009/03/13/napolitanos-remarks-national-fusion-center-conference.

168 "What's Wrong With Fusion Centers," ACLU, last accessed Oct. 24, 2022, https://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf.

169 Perez, Goodwin, & Quiason, "21st Century Policing," 15; Dia Kayyali, "Why Fusion Centers Matter: FAQ," EFF, Apr. 7, 2014, https://www.eff.org/deeplinks/2014/04/why-fusion-centers-matter-faq#12; Mark Harris, "How Peter Thiel's Secretive Data Company Pushed Into Policing," Wired, Aug.9, 2017, https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing.

170 Perez, Goodwin, & Quiason, "21st Century Policing," 15; "Get the BRIC Out of Boston," Muslim Justice League, last accessed Oct. 24, 2022, https://muslimjusticeleague.org/our-work/get-the-bric-out-of-boston; Daniela Hargus, Cristina Moreno, & Kennedy Barber-Fraser, "The Silicon Hills Have Eyes," Grassroots Leadership (2021): https://grassrootsleadership.org/sites/default/files/reports/silicon_hills_have_eyes_report_-_final_1.pdf, Alice Speri, The Defund Police Movement Takes Aim at Fusion Centers & Mass Surveillance," Intercept, Apr. 21, 2021, https://theintercept.com/2021/04/21/maine-defund-police-fusion-centers-mass-surveillance; Swan, "Law Enforcement Officials Brace."

171 "Federal Support For & Involvement in State & Local Fusion Centers," Permanent Subcommittee on Investigations (2012): 1 & 7, https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf.

172 "Letter on Inspector General Audit on SAR Program," STOP LAPD Spying, June 21, 2021, https://stoplapdspying.org/letter-on-ig-audit-of-sar.

173 "Suspicious Activity Reports & the Surveillance State: The Suppression of Dissent & the Criminalization of Arabs & Muslims in Illinois," Arab American Action Network and Policing in Chicago Research Group (2022): 2, https://aaan.org/media/cerp-report.

174 "Get the BRIC Out of Boston," Muslim Justice League.

175 Finbarr Toesland, "In An Era Of Data Sharing, Can A Real Sanctuary City Exist?," NextCity, Aug. 5, 2022, https://nextcity.org/urbanist-news/in-an-era-of-data-sharing-can-a-real-sanctuary-city-exist.

176 "Fusion Centers and Intelligence Sharing," Bureau of Justice Assistance, last accessed Oct. 24, 2022, https://bja.ojp.gov/program/it/national-initiatives/fusion-centers#:~:text=What%20Is%20a%

20Fusion%20Center,from%20a%20variety%20of%20sources.

177 "Fusion Centers: Issues & Options for Congress," CRS (2008): 4, https://www.everycrsreport.com/files/20080118_RL34070_685308a7155077c35f28662c-fa3d2b16daec7ff6.pdf.

178 "Fusion Centers: Issues & Options for Congress," 16.

179 "President's Homeland Security Advisory Council," CNN, June 12, 2002, http://www.cnn.com/2002/ALLPOLITICS/06/12/security.council.members/index.html; "Homeland Security Council," George W. Bush White House Archives, last accessed Oct. 24, 2022, https://georgewbush-whitehouse.archives.gov/hsc.

180 "Homeland Security Advisory Council: Summary of Meeting," DHS (2005): 4, https://www.dhs.gov/xlibrary/assets/HSAC_MtgSummary_121404.pdf.

181 "Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State & Local Information Fusion Centers," GAO (2007): 35, https://www.gao.gov/assets/gao-08-35.pdf.

182 "Fusion Center Guidelines," Department of Justice (2008): 16, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_guidelines.pdf.

183 "Federal Efforts Are Helping to Alleviate Some Challenges," 36 n.43.

184 "Federal Support For & Involvement in State & Local Fusion Centers," 13.

185 "Federal Support For & Involvement in State & Local Fusion Centers," 15.

186 "Fusion Center Locations & Contact Information," DHS.

187 "Fusion Centers in Illinois," ACLU; "LexisNexis Transformation Accelerates with Integration of ChoicePoint," LexisNexis.

188 "Microsoft & Illinois State Police Collaborate," Microsoft; "Microsoft Fusion Framework is an integrated, holistic technology architecture for fusion centers, which can help you to enhance information sharing and security by automating collection, intake, workflow management, collaborative analysis, data visualization, dissemination, auditing, and capture of business-performance metrics. (Microsoft, 2012)" quoted in Priscilla Regan & Torin Monahan, "Beyond Counterterrorism: Data Sharing, Privacy, and Organizational Histories of DHS Fusion

Centers," International Journal of E-Politics, no. 4(3) (2013): 8, https://publicsurveillance.com/papers/IJEP.pdf.

189 "Fusion Centers in Illinois," ACLU.

190 "Fusion Center Intelligence & Operational Software," Kaseware, last accessed Nov. 2, 2022, https://www.kaseware.com/government/fusion-centers.

191 Ng & Varner, "The Little-Known Data Broker Industry."

192 "Federal Support For & Involvement in State & Local Fusion Centers," 106.

193 "Statement of Mike Sena," National Fusion Center Association (2021): 4, https://www.hsgac.senate.gov/imo/media/doc/Testimony-Sena-2021-05-18.pdf.

194 "Statement of Mike Sena," 4.

195 "Chicago Budget Spreadsheet."

196 "FY 2020 HSGP Investment Justification: Boston Urban Area," DHS, 4, 5, 23, 25, & 71.

197 "LA FY2018 & FY2019 Projects," obtained through records request, https://drive.google.com/file/d/1lFHfIQnH58paShoFDIg7m8eZwLgLGZe-/view?usp=sharing.

198 "Extend the Term of Sole Source Contract Number 60701 With Palantir Technologies, Inc. to Provide Software Maintenance & Support," LA County Sheriff's Department, May 21, 2019, 2, http://file.lacounty.gov/SDSInter/bos/supdocs/135540.pdf.

199 "FY 2020 HSGP Investment Justification: Boston Urban Area," DHS, 4, 23, & 71.

200 "Chicago Budget Spreadsheet."

201 "LA FY2018 & FY2019 Projects."

202 Fernandes, "The Immigration-Industrial Complex," 175–77; O'Harrow Jr., "Introduction," 1–3.

203 "About," NFCA, last accessed Nov. 2, 2022, https://nfcausa.org/about.

204 "About," NFCA.

205 "Federal Support For & Involvement in State & Local Fusion Centers," 87–88.

206 "Statement of Mike Sena," NFCA, 4.

207 Tim Starks, "Post-9/11 Security Centers Now Face Budget Threats," CQ Weekly, July 30, 2011, http://public.cq.com/docs/weeklyreport/weeklyreport-000003920651.html.

208 Starks, "Post-9/11 Security Centers Now Face Budget Threats."

209 Dominic Lipinski, "Google-Backed Startup Uses Internet Ads to Counter Online Extremism," NBC News, Mar. 28, 2018, https://www.nbcnews.com/tech/security/google-backed-startup-uses-internet-ads-counter-online-extremism-n860961.

210 "Corporate Partner Program," NFCA, last accessed Nov. 2, 2022, https://nfcausa.org/corporate-partner-program.

211 Swan, "Law Enforcement Officials Brace for Potential Violence Around SCOTUS Draft Opinion."

212 Speri, "The Defund Police Movement Takes Aim at Fusion Centers & Mass Surveillance."

213 "About NHSA," NHSA, last accessed Nov. 2, 2022, https://www.nationalhomelandsecurity.org/about-nhsa.

214 "About NHSA," NHSA.

215 "2023 Exhibits & Sponsors," NHSA, last accessed Nov. 17, 2022, https://www.nationalhomelandsecurity.org/events/2023-exhibitors-sponsors.

216 "About NHSA," NHSA.

217 "Haystax Technology: A New Kind of Analytics and Cybersecurity Company," Hayxstax: 15, http://haystax.com/wp-content/uploads/2015/04/Corporate-Brochure.pdf.

218 "D2iQ," Koch Disruptive Technologies, last accessed Oct. 24, 2022, https://kochdisruptivetechnologies.com/portfolio-companies/d2iq.

219 "History," IJIS, last accessed Oct. 24, 2022, https://ijis.org/about/history.

220 "About," IJIS, last accessed Oct. 24, 2022, https://ijis.org/about/#board.

221 "IJIS Institute Sustaining Members," IJIS, last accessed Nov. 4, 2022, https://ijis.org/member-list.

222 "Partnerships," National Policing Institute, last accessed Oct. 24, 2022, https://www.policinginstitute.org/partnerships.

223 Law Enforcement Imaging Technology Task Force, "Law Enforcement Facial Recognition Use Case Catalog," IACP & IJIS Institute (2019): https://www.theiacp.org/sites/default/files/2019-10/IJIS_IACP%20WP_LEITTF_Facial%20Recognition%20UseCasesRpt_20190322.pdf.

224 "Fusion Center Guidelines: Developing and Sharing Information & Intelligence in a New World, Department of Justice (2005): https://www.ialeia.org/docs/Fusion_Center_Guidelines_for_Law_Enforcement.pdf.

225 "California Bay Area UASI TVTP. Promising Practices: Multiple Projects and Innovation Tracks," Department of Homeland Security (2021): 14, https://www.dhs.gov/sites/default/files/2022-05/EMW-2021-GR-APP%20-00083-Bay%20Area%20UASI.pdf.

226 "Glenn Archer," LinkedIn, last accessed Nov. 17, 2022, https://www.linkedin.com/in/glennlarcher; "Sabotaging Sanctuary: How Data Brokers Give ICE Backdoor Access to Colorado's Data & Jails," No Tech for ICE (2022): 7, https://notechforice.com/wp-content/uploads/2022/04/Sabotaging-Sanctuary_Final-Report_Design-4-1.pdf

227 Appris, "Appriss Insights Welcomes Glenn Archer as Vice President, Justice Intelligence," Global Newswire, June 30, 2020, https://www.globenewswire.com/en/news-release/2020/06/30/2055291/0/en/Appriss-Insights-Welcomes-Glenn-Archer-as-Vice-President-Justice-Intelligence.html.

228 "Membership," IACP, last accessed Nov. 2, 2022, https://www.theiacp.org/membership.

229 “About IACP,” IACP, last accessed Nov. 2, 2022, https://www.theiacp.org/about-iacp.

230 “IACP Technology Conference,” IACP, last accessed Nov. 17, 2022, https://www.theiacp.org/tech-conference#site-navigation.

231 “IACP Partner Program,” IACP, last accessed Nov. 17, 2022, https://www.theiacp.org/partners.

232 “IACP Technology Conference,” IACP.

233 Target, the national retail chain, is a major contributor and partner to several police foundations across the United States. “Police Foundations: A Corporate-Sponsored Threat to Democracy & Black Lives,” LittleSis & Color of Change (2021): https://policefoundations.org/wp-content/uploads/2021/10/Color-Of-Change-Report-Police-Foundations-A-Corporate-Sponsored-Threat-to-Democracy-Black-Lives.pdf.

234 “About IACP,” IACP.

235 “Department of Homeland Security,” IACP.

236 “Support for Sustainability of Fusion Centers,” IACP, Nov. 2, 2009, https://www.theiacp.org/resources/resolution/support-for-sustainability-of-fusion-centers; “Calling for Greater Collection and Dissemination of Information on All Crimes Through Fusion Centers,” IACP, Nov. 1, 2010, https://www.theiacp.org/resources/resolution/calling-for-greater-collection-and-dissemination-of-information-on-all-crimes; “Support of the National Network of Fusion Centers,” IACP, Nov. 19, 2014, https://www.theiacp.org/resources/resolution/support-of-the-national-network-of-fusion-centers,

237 “Policy Priorities for the 115th Congress,” IACP. https://www.theiacp.org/sites/default/files/all/i-j/IACPPolicyPriorities.pdf.

238 “Vincent Talucci,” Department of Homeland Security, last accessed Oct. 24, 2022, https://www.dhs.gov/medialibrary/assets/photo/29212.

239 “Vincent Talucci,” IACP, last accessed Nov. 3, 2022, https://www.theiacp.org/sites/default/files/2018-07/Talucci_0.pdf.

240 Mariame Kaba discusses defunding the NYPD to 50%. This is a step to making organizations like DHS obsolete and refunding basic community services. Mariame Kaba, “Yes, We Literally Mean Abolish the Police,” N.Y. Times, June 12, 2020, https://www.nytimes.com/2020/06/12/opinion/sunday/floyd-abolish-defund-police.html; This demand builds on calls in Just Futures Law’s Defunding the DragNet to reduce DHS’s budget for biometrics & surveillance networks by 50%. Dinesh McCoy, “Defunding the Dragnet,” Just Futures Law (2011): 8, https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/635c0a8119df2627cab1c567/1666976386334/JFL_Report-DefendingTheDragnet_111521.pdf.

241 “DHS Budget,” DHS.

242 See, e.g., Amanda Silberling, “Google Workers Protest $1.2B Project Nimbus Contract With Israeli Military,” Tech Crunch, Sept. 1, 2022, https://techcrunch.com/2022/09/01/google-workers-protest-1-2b-project-nimbus-contract-with-israeli-military.

243 See, e.g., “Librarians in Action: No Tech for ICE,” Mijente, last accessed Nov. 7, 2022, https://notechforce.com/librarians-in-action.

244 See, e.g., Ngakiya Camara & Kya Chen, “Students Are Pushing US Colleges to Sever Ties With Military-Industrial Complex,” Truthout, Nov. 7, 2021, https://truthout.org/articles/students-are-pushing-us-colleges-to-sever-ties-with-military-industrial-complex.

245 Preparedness Grant Effectiveness Case Study: New York City,” NPAD.

246 “Mayor de Blasio Testifies Against Cuts to Vital Anti-Terror Funding.”

247 “Professional Services Agreement: Contract No. 1650-15538,” Cook County.

248 “Public Safety Committee Report,” L.A. City; “FY16-20 LAPD UASI Funding.”

249 “FY 2020 HSGP Investment Justification: Boston Urban Area,” DHS, 34.

250 “FY16-20 LAPD UASI Funding.”

251 Grimm, “Activists Call for City to End Contract with ShotSpotter.”

252 “FY 2020 HSGP Investment Justification: Boston Urban Area,” DHS, 11.

253 “FY16-20 LAPD UASI Funding”; “US9129219B1,” Google Patents, last accessed Nov. 7, 2022, https://patents.google.com/patent/US9129219?oq=inassignee; Ali Winston, “Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policing Technology,” Verge, Feb. 27, 2018, https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd.

254 “Extend the Term of Sole Source Contract,” LA County Sheriff’s Department, 2.

255 “NYC OEM UASI Vendor List”; “Email from FOIL Officer at OEM.”