Meet Three Corporations Profiting Off Homeland Security

Over the last 20 years, tech corporations have fueled and profited off the US government's global War on Terror, abroad and in our neighborhoods. Corporations have made themselves indispensable partners to the Department of Homeland Security's (DHS) ongoing targeting of immigrants, Muslims, and Black and Brown communities.

After 9/11, corporations helped build the backbone of DHS's systems and influenced homeland security policy, driving demand for their products using counterterrorism justifications. Today, many of these same companies make millions by selling policing and surveillance technologies to local, state, and federal law enforcement. Corporations simultaneously support and fund law enforcement associations and think tanks, actively helping create the policies that keep them in business with the military and policing agencies.

Many of these tech corporations are household names and sell technologies we interact with on a daily basis, whether we realize it or not. They market themselves as working for the public good, while they collectively make billions in revenue through DHS and government contracts for policing and surveillance that endanger our communities. It's time we get to know the full picture.

There are thousands of corporations that benefit from homeland security funding and policy. Let's meet three of them.

Check out our report, ***DHS Open for Business***, to learn more about the role of corporations in expanding policing and surveillance in our communities and the DHS funding streams (like the Urban Area Security Initiative, or UASI) that provide millions in contracts for their products.

SURVEILLANCE RESISTANCE LAB

ACRE ACTION CENTER ON RACE & THE ECONOMY

MJL Muslim Justice League

LittleSis

MediaJustice

LexisNexis: The legal and research database—whose parent company also extracts and sells our personal data to police and ICE.

Data broker firms like LexisNexis/RELX 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.

LexisNexis, a subsidiary of RELX, is known for making research products for journalists and lawyers, but is also a **data broker firm** that profits from selling people's most intimate data. Today, LexisNexis makes millions off contracts with ICE and DHS, providing data on millions of people that powers ICE's deportations.

This is no accident. LexisNexis promotes its consumer data products as essential to counterterrorism and policing. After 9/11, LexisNexis and other companies began promoting their information technology services as a new "weapon" in the War on Terror. LexisNexis provided tools that enabled racial profiling of Arab and Muslim men, including Khalid Al-Draibi, a Saudi man who was falsely accused for involvement in the 9/11 attacks and deported from the US. In later publicity pitches for its "risk management" databases, LexisNexis emphasized its role in the Al-Draibi case, disregarding the false accusation at its core. LexisNexis also funded multiple studies after 9/11 that called for vastly increased data collection and sharing, which today is the backbone of the government's surveillance systems.

In the 2000s, LexisNexis grew its counterterrorism and policing products, investing in companies that enable invasive data collection, analysis, and mass data sharing while simultaneously stacking their affiliate boards of directors with law enforcement officials.

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.

LexisNexis also bought or invested in controversial companies known for privacy and civil liberties concerns, expanding its ability to extract and repackage consumer data for police, DHS, and **fusion centers**:

- In 2004, LexisNexis acquired **Seisint**, the company behind the information sharing system **MATRIX**, which was **pitched** as a counterterrorism product and was used to expand Islamophobic policing power through mass data collection and surveillance. **MATRIX "scored" people** based on their supposed terrorism risk, drawing interest from the federal government, and setting the stage for future data broker products that label people as threats.
- Seisint had built **Accurint**, which today is one of LexisNexis's key data sharing and analytics products, used by DHS, **ICE**, and in **fusion centers**.
- In 2008, LexisNexis's parent company bought risk management company **ChoicePoint**, which became integral to fusion centers as well as police information sharing.
- RELX's venture capital wing invested in **Palantir**, a data mining company that sells predictive policing software to police and fusion centers. Mijente and other organizations have highlighted Palantir's **role in ICE's deportation machine.**

LexisNexis's increasing control of our personal data set the stage for the company to become a key partner for DHS and police across the country. Today, LexisNexis **states** it has data contracts with 70 percent of local agencies and almost 80 percent of federal agencies.

Check out this map *from LittleSis that shows the connections between LexisNexis, government actors, and industry associations.*

Microsoft: The technology company building our software and computers—and the NYPD's real-time surveillance system.

Microsoft sells more than just our everyday computers; in the aftermath of 9/11, Microsoft became a key player in driving homeland security policy and directly lobbied DHS for contracts. Today, Microsoft is a central cloud computing provider to DHS and other policing agencies across the federal government, and regularly partners with local police departments to build up their surveillance systems.

In 2012, the NYPD and Microsoft jointly announced their partnership to build the Domain Awareness System (DAS), which was funded by at least $488.8 million in counterrorism grants from DHS (including the Urban Area Security Initiative program or UASI). 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. While city officials justify the system using counterterrorism rhetoric, DAS has repeatedly been used to target Black and Brown New Yorkers and is an increasing concern to public defenders and civil and immigrants rights groups in the city.

Today, Microsoft is a central cloud computing provider to DHS and other policing agencies across the federal government and secured over $266 million in contracts with DHS from 2011 to 2020.

Check out this map from LittleSis that shows the connections between Microsoft, government actors, and industry associations.

Motorola Solutions: The telecommunications giant that sells us our phones—and also helps police lobby for its surveillance products.

Motorola is known for making cell phones, modems, and radios, but its split off company, Motorola Solutions, is a huge **proponent and producer of policing and surveillance technology**, generating millions in contracts. It also owns **Vigilant Solutions**, a key provider of **automatic license plate reader (ALPR) technology and massive license plate databases**, police and **ICE** use to track drivers' movements historically and in real time. Motorola Solutions helped establish the DHS counterterrorism funding streams, promoting **"communications interoperability"** for law enforcement and the need for federal counterterrorism grants like UASI to fund them.

Motorola Solutions actively **advertises** its products as eligible for DHS counterterrorism funding, regularly hosts webinars for local officials on how to take advantage of grants, and supports the grant process—sponsoring services like **PoliceGrantsHelp.com**, making it easier for police to apply for grant programs like UASI to buy their technology.

Motorola **lobbies** the federal government to expand funding for DHS, which is deeply connected to their revenue streams. They are a sponsor of or conference exhibitor with three out of four policing associations we profiled in our **DHS Open for Business** report, giving it access to the key decision makers on policing federally and locally.

This approach has results: Between 2016 to 2020, the Los Angeles Police Department budgeted over $24 million in UASI funds to upgrade its radio systems, historically **provided by Motorola Solutions** (see our **records requests**). In 2016, Chicago signed a **five-year $25 million contract** with Motorola Solutions paid in UASI funds.

Check out this map from LittleSis that shows the connections between Motorola, government actors, and industry associations.

Fighting Back

How are communities fighting back against corporations like this? Where can you get involved?

- The #NoTechforICE campaign—led by Mijente, who partners with organizations like Just Futures Law and the Surveillance Resistance Lab—calls on LexisNexis, Thomson Reuters, and other companies to stop providing services that facilitate the detention and deportation of immigrants and end all contracts with ICE.
- Inspired by #NoTechforICE, #NoTechforApartheid is a campaign led by MPower Change and Jewish Voice for Peace demanding that Amazon and Google cancel their contracts supporting Israeli apartheid and the surveillance and targeting of Palestinians.
- The Stop ShotSpotter coalition has been organizing in Chicago and nationwide to end city contracts for the gunshot detection technology.
- The Athena for All coalition fights back against Amazon's harms to workers, immigrants, and communities of color, and demands that cities cancel their data sharing partnerships with Amazon's Ring for its harms to BIPOC communities.

SURVEILLANCE RESISTANCE LAB
ACRE ACTION CENTER ON RACE & THE ECONOMY
MJL Muslim Justice League
LittleSis
MediaJustice