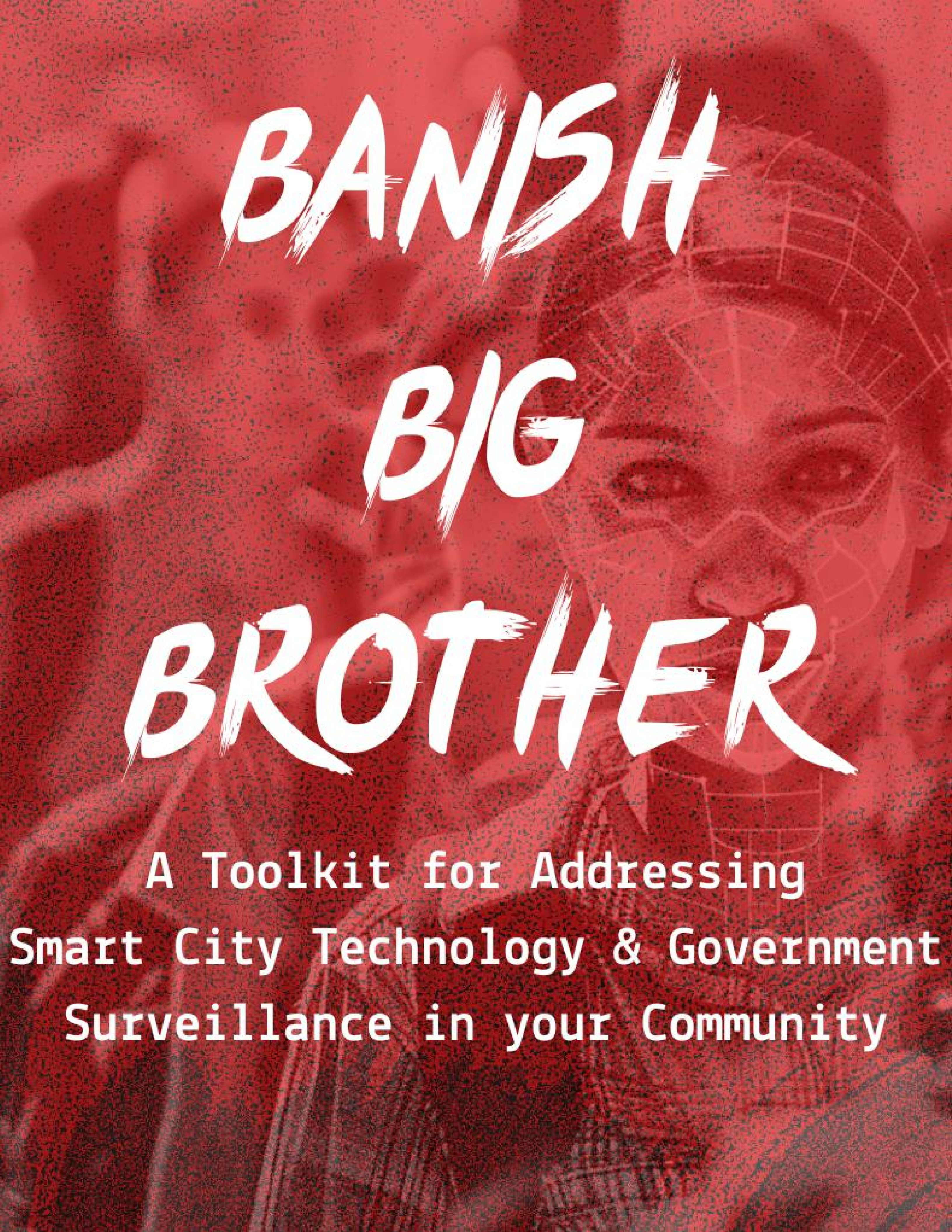
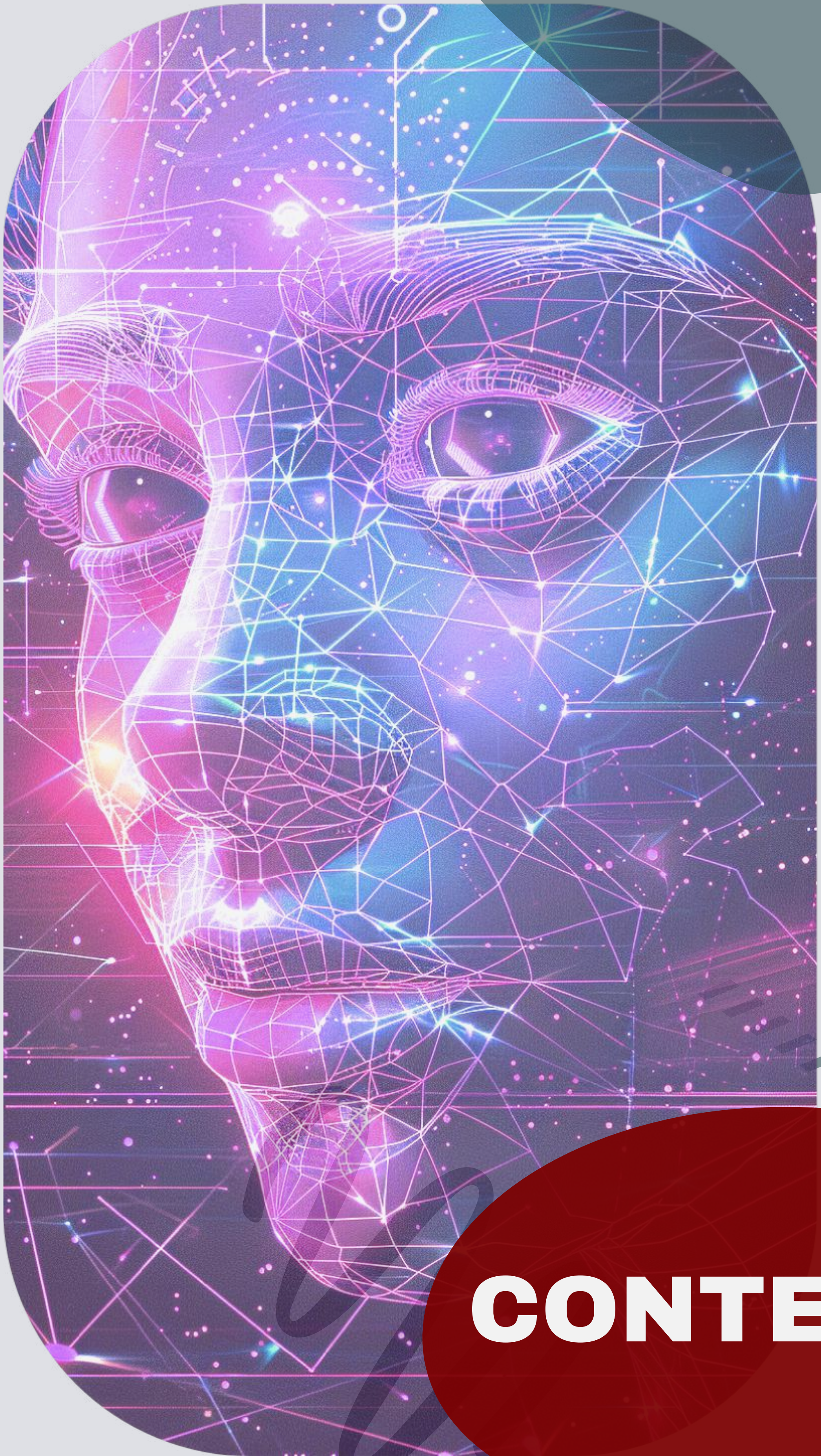


BANISH BIG BROTHER

A Toolkit for Addressing Smart City Technology & Government Surveillance in your Community

WHAT'S INSIDE



CONTENTS

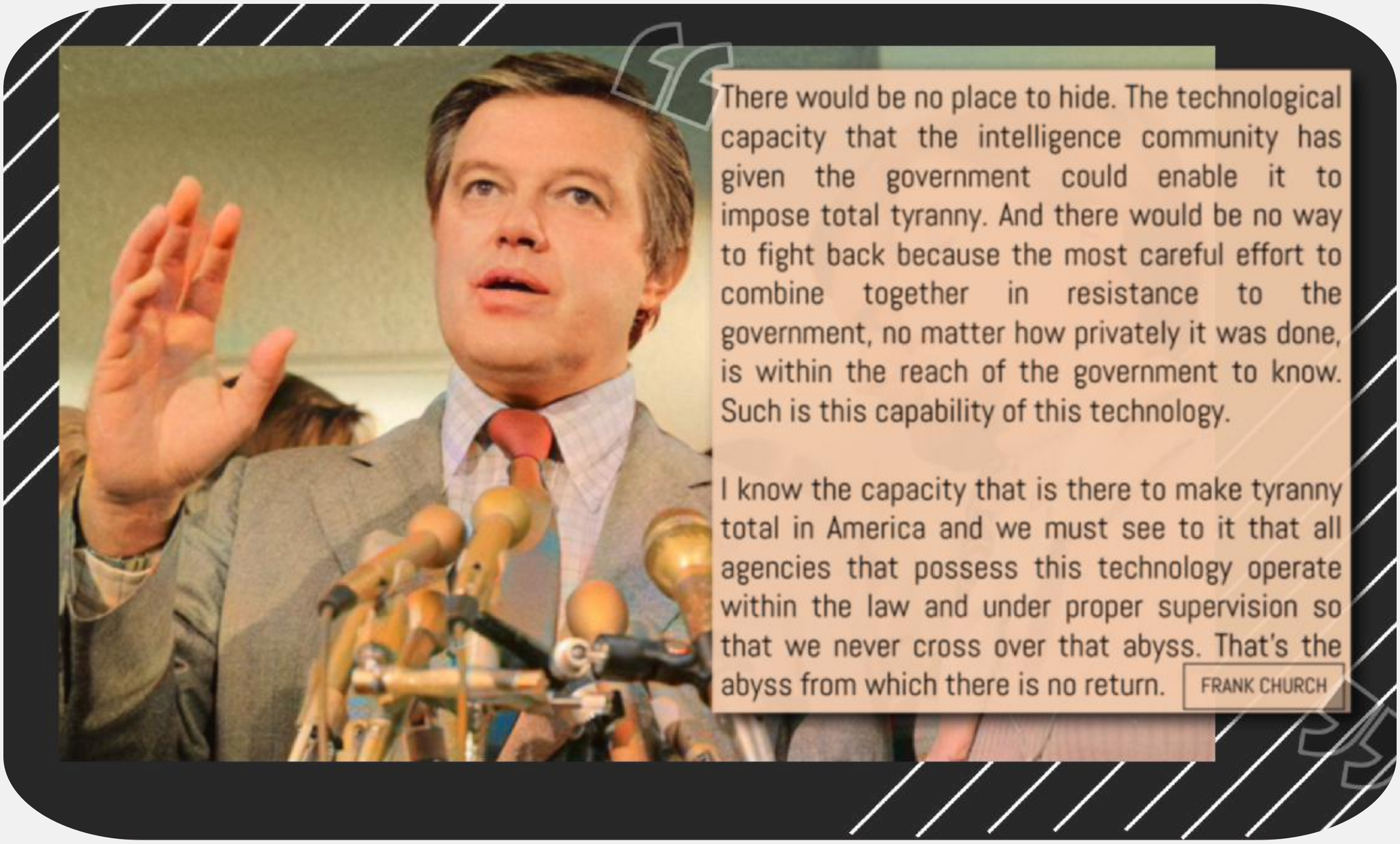
CHAPTER ONE

"SMART" CITIES IN AMERICA

"Technology is a useful servant but a dangerous master."

– Christian Lous Lange

Across the country, and the globe, there is a movement to transform urban areas into "smart" cities. Although a marriage of technology with city life and administration is obvious, knowledge of what "smart" actually means is often not. This toolkit aims to provide Banish Big Brother members and chapters with a deeper understanding of these initiatives and an action plan for addressing the transformation of your own city.



There would be no place to hide. The technological capacity that the intelligence community has given the government could enable it to impose total tyranny. And there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is this capability of this technology.

I know the capacity that is there to make tyranny total in America and we must see to it that all agencies that possess this technology operate within the law and under proper supervision so that we never cross over that abyss. That's the abyss from which there is no return.

FRANK CHURCH

CHAPTER TWO

What is a "Smart City?"

"What gets measured gets managed."

– Peter Drucker

Smart cities use a combination of embedded cameras and sensors to collect data and then employ artificial intelligence (AI) to process that data to make decisions and trigger actions. This is done by creating a "digital twin" of the city through which every static element, movement, condition, and interaction is accounted for, measured, and recorded.

Data can be collected through the following methods:

1. Cameras—Cameras are deployed throughout the city, using facial recognition software to personally identify and monitor pedestrians. (Clearview AI)
2. GPS—Cell phone data is intercepted to track the movements of the owner. (X-Mode)
3. Automated License Plate Readers (ALPR's)—License plates are automatically scanned, identified, and tracked throughout the city. (Flock TALON)
4. Audio Sensors—Audio waves are detected and analyzed. (ShotSpotter)
5. Thermal Sensors—Heat is measured to determine presence and temperatures of pedestrians.
6. Environmental Sensors—Data related to environmental conditions such as weather, water levels, and air quality is collected.
7. Motion-Detection Sensors—Record the presence of pedestrians or cars by detecting physical activity.
8. Connected Devices—Private devices such as personal cell phones, cloud-based security cameras, wearables, and utility meters are connected to smart city infrastructure.

These devices are often attached to "smart poles" or drones. Although many of these cameras and sensors are on public property, many municipalities have relationships with cloud-based services that also allow access to data collected by private devices.

Once the data is collected, it is processed by artificial intelligence and the results are used to achieve a number of goals. These goals are typically focused in the areas of efficiency, safety, and convenience.

You might spot an automated license plate reader like this mounted on police vehicles, traffic lights, road signs, or as stand-alone installations.

CHAPTER THREE:
WHAT ARE THE THREATS TO LIBERTY?

“Just imagine North Korea in twenty years when everybody has to wear a biometric bracelet which constantly monitors your blood pressure, your heart rate, your brain activity—24 hours a day. You listen to a speech on the radio by the Great Leader, and they know what you actually feel. You can clap your hands and smile but if you’re angry, they know.You’ll be in the gulag tomorrow morning.”

– Yuval Noah Harari

The potential benefits of smart city technology are often touted to promote acceptance and adoption but there are many drawbacks and dangers to civil liberties.

There are different levels of data that are collected by these devices. On one end of the spectrum are those that make measurements of environmental conditions such as weather or detect the presence of vehicles or pedestrians through motion-detection. On the other end of the spectrum are data collection practices such as facial recognition and license plate scans that collect data that is personally tied to identified individuals. While those technologies that collect more generalized data may ultimately erode privacy, it is those which link data to individuals which pose the gravest threats.

Some ways in which these technologies pose threats to liberty include:

1. Stalking by government—Smart city surveillance and stalking have many common features. This type of monitoring goes beyond simply capturing images of citizens who happen to be out in public. Individuals are personally identified through facial recognition or license plate scans and their movements throughout the city and interactions with others are compiled and recorded for an indefinite (perhaps permanent) period of time. This creates an intimate picture of the daily lives of every citizen without requiring consent.

2. More than just surveillance—Sensors, cameras, and software can capture more than just images and identification data. Facial recognition capabilities can include reading mood and tracking eye movements to make generalizations about likes, dislikes, sexual preferences, physical health, and behavior. Heat sensors can take temperatures and audio sensors can often record private conversations. Advanced AI can recognize individuals by their gait as well as mathematical formulas representing body measurements and proportions.

3. Who owns the data and what they are doing with it—There is an alarming lack of regulation and oversight regarding what happens to smart city data. Most smart city initiatives are powered by technologies provided by private corporations. These corporations can capture data to sell or use without limitation.

Sharing or selling data to other corporations can have a negative impact on consumers. An example of this might be sharing lists of citizens who make frequent visits to liquor stores or bakeries to negatively impact their health or auto insurance rates. Monitoring the behavior of individuals, such as what they are looking at, can make them subjects of targeted marketing campaigns and propaganda.

Improper handling of such data can expose private citizens to such dangers as political intimidation or physical harm from those with ill intent. Data breaches can put citizens at risk from both domestic threats and foreign adversaries. Citizens have no access, ownership, or control over their personal data.

4. The “chilling effect”—When people are aware that they are being watched but unsure when or where, they will begin to behave at all times as if they are being watched (panopticonism.) This creates an atmosphere of intimidation that can lead to alteration of one’s behavior based on the possibility of perception and erode freedom of participation in perfectly legal activities, such as protest.

5. The “mosaic effect”—Although a piece of information on its own may not diminish privacy, when it is combined with other pieces of information it can pose a threat. As different databases are combined under digital ID systems, the addition of smart city data serves to fill out a more complete picture that reveals an intimate portrait of people’s lives

6. Asymmetries of power—Personal data is accessible by a few people in positions of power while the data of those in power remains inaccessible to those that they observe. This creates opportunities for abuse by an elite minority who are themselves protected from scrutiny.

Panopticon:
A circular
prison enabling
unseen surveillance
from a central point.

7. Erasure of personal accountability—Currently, law enforcement, government employees, and politicians are expected to justify their actions with facts. Tying decision-making to AI creates opportunities to avoid accountability by blaming the data.
One example of this is the use of algorithms in making decisions in child protective services cases. In other words when asked, "why did you do that?" the response might be, "because the data said to" rather than providing an articulable reason.

8. Power in the hands of the worst possible government—Technology identical to that employed in smart city programs is being used by totalitarian governments, such as Myanmar and China, to commit genocide, execute activists, and oppress its citizens through social credit systems.

BANISH BIG BROTHER PODCAST

hosted by Elizabeth Melton and Zach Varnell

Join hosts Elizabeth and Zach as they embark on a thought-provoking journey through the labyrinth of privacy, technology, surveillance, and the digital age's unseen battles. Banish Big Brother isn't just another podcast; it's a mission to unravel the complex web of information that surrounds us, challenge the omnipresent eyes of surveillance, advocate for the sanctity of personal privacy in a world that's growing increasingly transparent, and have fun doing it.

BanishBigBrother.com/subscribe

CHAPTER FOUR: PRIVACY & STATE LAW

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying that you don't care about free speech because you have nothing to say."

– Edward Snowden

In 1905 the Georgia Supreme Court made a consequential ruling in the case Pavesich v. New England Life Insurance Co. et al. Although this case was waged by an individual against a private business, the court ruling expresses significant findings that broadly define a right to privacy.

Here are some highlights of this ruling that are applicable to smart city technology and government surveillance:

1. Just because a right is not documented in law or precedent, does not mean that the right does not exist. Therefore, if a right to privacy is not documented, that does not mean that there is no right to privacy.

2. The right to privacy is embodied within natural law and "embraced within the absolute rights of personal security and personal liberty."

3. Personal security does not simply mean that one has a right to exist. It also means that one has a right to enjoy one's life while existing. When one is deprived of things, such as privacy, that are necessary to the enjoyment of life it is an invasion upon one's rights.

4. Personal liberty does not simply mean that one is free of physical restraint, it also means that one has the right "to be let alone" and to determine if one's mode of life "shall be a life of publicity or privacy."

5. One exception to this right is that one who seeks or holds public office waives their right to privacy to the extent that they cannot restrain or impede investigation into their private life which might "throw light upon the question as to whether the public should bestow upon him the office which he seeks." A holder of public office "subjects his life at all times to closest scrutiny, in order that it may be determined whether the rights of the public are safe in his hands."

Essentially, items put forth in this ruling indicate that the public has a right to privacy but government officials do not. The surveillance technologies used in smart cities create an environment in which the opposite occurs—the people have no privacy but government officials do. This precedent provides a foundation for opposition to the surveillance and personal-identity components of smart city projects.

If you are using this toolkit for activism outside of Georgia, research privacy laws and court rulings in your state to determine possible avenues for opposition.

Digital Twins

A digital twin is a virtual replica of a city's physical assets, infrastructure, and systems. It uses real-time data collected from sensors, cameras, GPS devices, and other IoT (Internet of Things) technologies to create a dynamic, constantly updated model that reflects the current state of the city. This virtual representation allows city planners to simulate, analyze, and attempt to manage operations and services.

While digital twins aim to enhance the management and efficiency, they also raise privacy considerations. The extensive data collection involved can include personal information and tracking of individuals' movements and activities.

CHAPTER FIVE: RESISTANCE IN YOUR COMMUNITY

"It's a brilliant method of social control that only in the extreme cases needs imprisonment and otherwise simply controls people on the basis of data…This is where we are going if we don't control it."

– Ken Roth, Human Rights Watch (referring to the Chinese social credit score system)

The answer to the problem of this kind of surveillance and control begins in your local community.

Here is an outline of steps to get your resistance movement started:

1. Form a Digital Surveillance Opposition Team—Although an individual can take on a project such as this, you stand a greater chance of success by forming a team. Having a group of members from your Banish Big Brother chapter is a good idea, but consider bringing in people from the outside who are dedicated to the cause. It is good to have people with a variety of strengths such as writing, research, interpersonal communication, public speaking, and technological expertise.

2. Collect information—The first task that your newly formed team should complete is to find out as much information as possible about the technology that your city has implemented or plans to implement. There may be some information available on the official city website or in local media articles. You may also find cooperative individuals in your city's tech division, though they have a vested interest in not being forthcoming with information. For a complete picture, you may need to submit an Open Records Request or Freedom of Information Act (FOIA) request. You can find instructions on how to do this in the Resources section of the toolkit.

3. Educate your team—Read articles, watch videos, and attend presentations to become experts in these technologies and, more specifically, how they are being used in your community. See the Resource section at the end of this document to get started. Be prepared to answer questions confidently and know where to direct people for more information.

4. Educate the public and gather allies—As the benefits of smart city technologies are promoted but not the harms, the majority of the general public is completely unaware of the scope of the intrusion that these technologies pose. Create social media groups and materials, such as brochures, that inform the public of your efforts. Set up educational presentations both for the general public and for targeted groups and notify the local media of these presentations. Check out documents, presentations, and other resources available on the Banish Big Brother website. New items are added on a regular basis.

your own presentation. Different groups and demographics will have different considerations so it is helpful to create multiple presentations that will highlight a variety of concerns.

If you are reluctant to give the presentation, contact Banish Big Brother. We may be able to give a presentation for you or train members of your team. Just reach out at team@banishbigbrother.com.

As you make these presentations, gather allies among the various groups with whom you share information on this focused issue. This subject is relevant to citizens across the political spectrum and from all walks of life. Do not hesitate to include members of groups that you might normally consider to be adversaries. The more widespread your support, the greater the impact of your opposition. The most important goal is to stop the abuse of the technology regardless of the motivations for doing so. These concerned citizens can become members of your team or, if they have large numbers, form their own teams with which your team can collaborate.

Here are some suggested groups with whom to network, along with recommended approaches:

A. Pro-freedom groups—Local groups that espouse individual rights and freedom or that have opposed lockdowns and mandates will generally be in alignment with smart city opposition without having to create a targeted presentation. This can include libertarian-leaning groups outside of official party affiliations, Tea Party groups, Constitutionalists, and others.

B. Second Amendment advocates—This type of surveillance can have a negative impact on the exercise of Second Amendment rights. Citizens can be surveilled while visiting gun stores and gun shows. Technology can capture video of people who are carrying openly or carrying concealed but “printing.” Certain technologies can detect the presence of firearms without capturing on video (ZeroEyes, PatScan). Even if carrying or purchasing weapons is being done legally, this data can be stored and used to identify and target people at a future time. With little oversight as to how the corporations that provide the technology store or share the data, there is the possibility that it could be sold or shared to corporate partners such as health insurance companies resulting in a negative impact to consumers.

C. Churches and religious groups— In many countries where certain religions are banned, those practices have remained alive for decades because they have taken place underground. While it seems unlikely that such a scenario would happen in the US, many remember that worship services were forbidden in many places throughout the country during lockdowns and pastors were arrested for openly defying those mandates. At certain times of political turmoil, people attending particular religious services, such as mosques, have been targeted. In a country where a religion may be brutally repressed this level of surveillance would make defiance impossible.

D. Criminal justice reform groups—Smart city technologies perpetuate the harassment of people for violations of victimless “crimes” and revenue-generating activities while sophisticated criminal enterprises run by connected individuals can remain undetected or ignored.

E. NAACP and other equality groups—Surveillance technologies can be used to specifically target particular demographics according to race and sexual orientation. Facial recognition software has been refined to the point that it can determine someone’s sexual orientation based upon eye movements, heart rate, and breathing, making those in the LGBTQ+ demographic particularly vulnerable in areas where they may be targeted.

F. Other political organizations—All other political party affiliations and groups—Republican, Democrat, People’s Party, Constitution Party, Green, etc.—have an interest in opposing this type of digital surveillance. When talking with these groups simply focus on the issues listed in this guide that are in line with their party.

G. Pro-choice advocates—Some legislation aimed at limiting choice has proposed prosecution of those seeking abortion in other states as well as those who might assist them, including drivers. This kind of digital surveillance can put together a scenario which would aid in that prosecution. This might include a trip to a pharmacy for a pregnancy test followed by a trip out of town. As surveillance and tracking data are stored for indefinite periods of time, those seeking legal abortion could later be targeted when political conditions change.

H. Anti-corporate activists—Smart cities are fueled by corporate interests. Corporations make substantial sums from sales of the technology and hold valuable data with few restrictions on its use.

I. Privacy and cyber-security advocates—Apart from the obvious privacy concerns, individuals have no control over what happens with their own data.

J. Government officials—Historically, in repressive governments elites are targeted for surveillance to a higher degree than the general population. This is not only bad for the elites themselves but also for the population as it can lead to corruption through blackmail. In Georgia, the Pavesich v. New England Life Insurance Co. case makes the personal data of government officials a target for lawsuits or Open Records / FOIA requests.

K. Small businesses—Surveillance is bad for business. Businesses that offer products and services that patrons would be reluctant to have publicly shared such as bars, night clubs, liquor stores, adult novelty shops, gun stores, and those offering medical procedures of a sensitive nature are a good place to start.

L. General arguments for all groups—The overarching message with any group should be that this type of tracking and monitoring needs to be prohibited rather than perfected. For example, if facial recognition tends to misidentify people of color the answer is not to better identify people of color. A consistent point to make is that we never know who will be in charge or how the government might be oriented. Just because one's preferred party might be in charge now does not mean that one's rival party will not be in charge later. It is important to drive home the idea of this power resting in the hands of the worst-possible government.

5. Approach your city government—Try to determine who among your city's representatives might be inclined to support restrictions on surveillance. Research the voting records to discover which councilors voted against regulations that compromised freedom. If your local government has a video channel, watch videos of meetings in order to identify which councilors prefer a more libertarian approach to governance as opposed to those who prefer heavy-handed government intervention.

Contact promising candidates to arrange an in-person meeting with members of your team. If you cannot arrange a meeting, try to arrange a phone call. If a personal conversation cannot take place, send an email. The goal is to get councilors who would be sympathetic to smart city intervention to support the cause before addressing the entire council in an official meeting.

These initiatives are often funded in the form of grants which are offered through educational institutions or corporate partners (i.e. Georgia Tech offers grants in Georgia and Alabama Power offers grants in Alabama). In many cases, even the government representatives who are voting for these systems are not aware of how these technologies work. They simply know that the grants offer perks, such as public Wi-Fi, to their local populations that do not require expenditure of local funds. In your in-person meeting or other communication, your first task will be to educate those representatives on the dangers that these unregulated projects pose and express your desire to impose restrictions, remove troubling aspects of the technologies, or deny projects.

Provide these representatives with a proposal for a resolution. You can find a template for this proposal on the Banish Big Brother website. Be sure that your approach is polite, professional, and cooperative rather than combative. You can always escalate to a more uncompromising approach later if a good-natured approach does not work initially.

After mobilizing sympathetic representatives, make your case to the entire council at a public meeting. Most council meetings offer a speaking opportunity lasting from two to five minutes. Choose a well-spoken team member with executive presence to address the council. There is a template for a five-minute presentation in the resources section of this toolkit that you can use as a basis. Emphasize the dangers that these technologies pose personally to them and their families as well.

What do we do if our city representatives are not sympathetic to our cause?—If your pleas for sanity fall on deaf ears, do not give up!

These are additional steps to consider after your city council presentation:

A. Continue speaking to local citizens and growing your numbers. The larger your movement becomes, the more powerful it becomes.

B. Continue appearing at city council meetings. Have members of allied groups rotate speakers.

C. Organize a phone call campaign of concerned citizens to representatives.

D. Investigate waging a lawsuit for violation of privacy using Pavesich v. New England Life Insurance Co. (or, if you are not in Georgia, other privacy precedents or statutes) as the basis of your suit.

E. File an Open Records or FOIA request asking for the data of your public officials.

F. Stage a peaceful protest.

G. Make your voices heard through editorials, media interviews, blog posts, social media posts, signs, podcast appearances, and other outlets.

H. Organize boycotts of areas that are known to have particularly heavy surveillance, such as “downtown” or business districts.

CHAPTER SIX

Creating a Movement

“The world is a dangerous place, not because of those who do evil, but because of those who look on and do nothing.”

– Albert Einstein

Resistance to digital surveillance starts in your city but shouldn’t end there. In an effort to “keep up” with what other cities are doing, local politicians are often swayed by broader movements that are deemed to be popular.

To make your local movement a broader movement:

A. Network with groups and individuals in other cities who are also working on this issue. Connection with others provides much-needed moral support and allows you to share effective techniques.

B. Lobby your state and federal representatives to secure privacy-centered legislation on the state and federal levels.

C. Take advantage of every opportunity to educate others. The insidious aspect of this issue is that it is, in many ways, invisible. People are unaware of the digital surveillance and even many that are aware do not fully understand how intrusive it is.

D. Keep the privacy ideal alive—It is crucial that we foster a mindset that values privacy. Many have resorted to accepting defeat by entertaining the notion that privacy is dead and that we might as well accept it. It is imperative that we counter that mindset, both in ourselves and others, and promote the concept of privacy as a cherished right of which protection is a goal that is worthy of endeavor.

CHAPTER SEVEN: MAKING A DIFFERENCE ON A PERSONAL LEVEL

“No snowflake in an avalanche ever feels responsible.”

– Stanislaw Jerzy Lec

If you are not ready to launch a coordinated effort or if you want enhance the effectiveness of your opposition team, there are things that we can do on a personal level to resist the advancement of digital surveillance:

A. Reduce the data that you produce—These systems are fueled by data and any data of which they are deprived makes a difference. Some ways that you can reduce data collection are simple.

Every time that you use cash or write down directions instead of using GPS you are making a stand for privacy. Wearables that collect vital health measurements such as blood pressure or heart rate can be avoided. If you simply must use them, avoid allowing your information to be transferred to a cloud. Any cloud-based technology—from doorbells and other security systems to storing your personal files and photos—can instead be transferred to closed technologies that you control. Refuse to participate in programs promoted by law enforcement that ask you to voluntarily register your private security system with their agency.

Turn off any computerized systems on your vehicle that can be turned off. Even covering a camera sensor on your personal vehicle or computer with a piece of tape makes a difference.

B. Make a statement—Realistic 3D printed masks, different makeup techniques, and clothing that mimics faces or license plates have been designed to try to thwart license plate readers and facial recognition. The effectiveness of these is limited and, as AI is perfected to identify people by gait and body measurements, they become more limited. Wearing them, however, is a powerful form of protest and is a good way to start a conversation about smart city technologies and digital surveillance.

C. Choose analog—There is a current trend of making choices that fall outside of the computerized world. From pen and paper journaling, to old-school watches, to blind dates set up by friends—many, particularly those of the youngest generation, are choosing to embrace the solutions of the past rather than to run willingly into a dystopian future. Technology, in some form or other, is here to stay but that does not mean that it must our lives completely. There are many ways in which we can remain connected to the real world as opposed to the virtual one.

D. Keep the privacy ideal alive—It is crucial that we foster a mindset that values privacy. Many have resorted to accepting defeat by entertaining the notion that privacy is dead and that we might as well accept it. It is imperative that we counter that mindset, both in ourselves and others, and promote the concept of privacy as a cherished right of which protection is a goal that is worthy of endeavor.

SMART: coming to a city near you
A Gray Matter Productions film

Have you noticed them? Cameras, sensors, and license plate readers are quietly appearing everywhere—city streets, rural roads, and public spaces worldwide. What does this rapid deployment mean for our future? Are we on the brink of a technological utopia offering unparalleled safety, efficiency, and convenience, or is there a darker side to these advancements?

Join us as we delve into these pressing questions in our groundbreaking documentary series, ***SMART: Coming to a City Near You***. Featuring insights from Derrick Broze of the Conscious Resistance Network, Mike Maharrey of the 10th Amendment Center, technical expert Aman Jabbi, and privacy advocate James Dutton, we uncover the realities behind the smart technology revolution.

The documentary is out now!

Check it out on **thegraymatterproject.substack.com** and please consider supporting this important project. Don't miss it!

CHAPTER EIGHT: RESOURCES

Banish Big Brother Podcast:
BanishBigBrother.com/subscribe

Banish Big Brother Blog:
BanishBigBrother.com/blog

Sample City/County Council Speaking Script:
https://banishbigbrother.com/2024/06/sample-city-county-council-script/

Filing an Open Records or FOIA Request:

File Online:

- Visit https://www.muckrock.com.
- Search for the topic of interest first to see if the information is already available or to find a similar request for reference.
- File the request, specifying that the information is not for commercial use.

By Phone:

- Clearly articulate the exact documents you are looking for.
- Call the agency and request the information, citing your state's Open Records or Freedom of Information Act. Note that there will be no letter or online entry to prove your request.

By Mail:

- Address the letter to the head of the department or agency.
- Cite applicable Open Records or FOIA laws.
- Include the state's time limit for response, the information requested, and specify that it is not for commercial use.

Legislation Enacted by San Francisco Limiting the Use of Facial Recognition:
https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A

Action and Resources from ACLU:
https://www.aclunc.org/fighting-high-tech-government-surveillance

Just Cities Policing Technology Toolkit:
https://static1.squarespace.com/static/61e97b77bece8a66e53139cc/t/62151d6a14faa20f7e09b77f/1645550959288/2022.2.22_Just+Cities_Policing_FINAL.pdf

Whose Streets? Our Streets! Substack:
https://whosestreets.substack.com

Videos on Dangers of Smart City Technology and AI:

Adam Greenfield on the Dangers of Smart Cities
https://www.youtube.com/watch?v=L6z2S1Y1IgQ&t=903s

How to Survive the 21st Century | DAVOS 2020
https://www.youtube.com/watch?v=eOsKFOrW5h8&t=804s

Will the Future Be Human? - Yuval Noah Harari at the WEF Annual Meeting 2018
https://www.youtube.com/watch?v=npfShBTNp3Q&t=1194s

Hacking Humans - Yuval Noah Harari Roundtable at EPFL
https://www.youtube.com/watch?v=xhpXU0x5894&t=2870s

Smart Cities: A threat to liberty
https://www.youtube.com/watch?v=EK5yiqopw1Y&t=2096s

"Smart Cities" Are A Decoy... Call them "Spy Cities" - FGP#18
https://www.youtube.com/watch?v=a7W9yTuTZAc&t=1364s

The Grey Matter Project, Producers of SMART: Coming to a City Near You:
https://thegraymatterproject.substack.com/

EFF's Street-Level Surveillance Hub:
https://sls.eff.org/
