Fam, these are probably going to be some of the hardest years of our lives. And yes, it is going to get worse before it gets better.

Across the country we're all waking up and trying to understand what does the new administration mean for me. What will I lose, who else will be vulnerable, and yes, how can I fight.

At Equality Labs we believe we must begin the fight by understanding how we can fight safely, and how to protect ourselves and our communications.

We must also keep one another close, the strongest defense against Trump is a collective one rooted in community, self-care and accountability.

We have a president who is a **RAPIST, RACIST,** and **ISLAMOPHOBE**. He has done terrible, immoral things in his past, and now has the power to do many more.

Armed with a Republican-controlled Congress, we do not know how this administration will address protest. He is an unstable violent man who now has access to the destructive powers of the National Security Agency (NSA), the American military, and a nuclear arsenal.

THINK ABOUT THAT!

What comes next is beyond all understanding. There is no returning to the status quo. Our homes, our workplaces, our communities—even our families—will never be the same.

We must fight like our lives depend on it. **Because, in fact they do.**

This curriculum aims to present immediate common-sense measures to help activists learn how to protect each other and their movements.

While we are still unsure of what this change will bring, we should assume that surveillance and censorship will increase, and that the Trump Administration's tools and strategies will be more sophisticated than anything we've seen. These surveillance tools have existed for a while but were not used to their full potential under the previous Obama administration.

Additionally, we can expect that individuals fighting for progress will be targeted now more than ever before. While these prospects are overwhelming, the good news is that there are strategies and tools designed to help you avoid most surveillance successfully. We approach this new surveillance era with caution but also with Knowledge. This curriculum will help you make informed decisions about protective measures that can reduce your level of surveillance harm while helping you navigate new risks as they come up. There will never be a perfect silver bullet in terms of surveillance evasion but we believe we can help you feel safer as you organize because you know the

tools and you know your rights.

Trump's election campaign showed signs he would take the position of "erring on the side of (state) security" over people's rights.[1] We know that he has called for closing parts of the internet to protect against "Islamist propaganda".[2] He was also deeply critical of Apple over its refusal to unlock an iPhone implicated in a California shooting for the FBI.[3] And we can expect increased efforts to target Black and Brown communities using databases in predictive policing efforts that use algorithmic discrimination to go after those that are targets because they are "undocumented," "gang members," and/or— "criminals" regardless of whether or not such assumptions are true.

All of these issues must be considered in the context of Trump's majority in both houses of Congress. We know there will be members of his administration who will push harder than ever for "back doors" that allow the government to bypass data security measures like encryption. They can also easily expand the already bloated phone surveillance apparatus currently used by the NSA. Trump's words and actions have suggested that he would push for increased targeting of certain peoples. He has even suggested the creation of a "National Database of Muslims."[4] All of this has the tech world, legal, political experts, activists, and community members worried.

We also know many people in our diverse communities feel powerless and may even argue, "What's the point?" But, in fact, there are simple digital security steps you can take now to help protect you from most threats, and make the remaining threats very expensive for malicious actors to implement.

We hope this curriculum will create a foundation for an education in safety and resilience, and a pathway to bring this crucial conversation into your homes, organizations, and movements. Digital security is a process not a destination and we believe that together we can make all of us safer!

[1] http://www.cnn.com/2015/12/01/politics/donald-trump-nsa-surveillance/
[2] http://www.reuters.com/article/us-usa-election-cyber-idUSKBN13503H
[3] http://www.huffingtonpost.com/entry/donald-trump-apple_us_56c78150e4b0928f5a6bdd3e
[4] http://www.nytimes.com/politics/first-draft/2015/11/20/donald-trump-says-hed-absolutely-require-muslims-to-register/?_r=0

HOW TO USE THIS CURRICULUM

We hope this curriculum will arm you with basic digital security knowledge and effective, simple-to-follow pointers for staying safe. Read this material, come to the workshops, and refer to the curriculum whenever you need to. We will also be offering curriculum module updates at equalitylabs.org so visit us often!

THE CURRICULUM AND WORKSHOP SHOULD HELP YOU:

- Understand the history of surveillance in the United States
- Understand the basics of digital security
- Secure your phone
- Secure your computer
- Secure your network access
- Secure your browser
- Secure your identity
- Secure your social networks
- Secure your communications

LEGEND

This legend will help you identify the icons in this curriculum which highlight significant information.

NOTE: The pencil sign denotes important details that often will provide important background to comprehending the section at hand.

TIP: The lightbulb brings attention to important shortcuts or key concepts to help you make a task easier and faster or even both.

WARNING: When you see the warning sign, take note. These important notes stress actions to avoid that could make you vulnerable. These notes could also include actions that can keep you safer.

TASKS: When you see this checkmark you should be aware that you are being introduced to a key step that must be completed to ensure the security process being discussed is implemented correctly. Do not proceed to the next security task until you have completed the checkmark at hand as many steps are interdependent of each other.

WHERE DOES THE U.S. STAND ON DIGITAL SECURITY ISSUES TODAY?

THE RIGHT TO PRIVACY

The right to privacy is a powerful and necessary foundation of democracy. When the right to privacy is connected to the right to free speech and the right to assemble we have the three fundamental pillars of any functioning democracy. When any one of these pillars are compromised, democracy itself is at risk.

The right to privacy is our right to keep a domain around us. These domains include all those things that define our individuality, such as our bodies, home, property, thoughts, feelings, secrets, and identities. The right to privacy gives us the ability to choose which parts of these domains, others—most importantly, state and corporate entities— can access and empowers us to control the extent, manner, and timing of this use.

If a government strips us of privacy in our lives and in our communications, it can halt thoughts, innovations, movements, and political actions that differ from the mainstream. The feeling of being watched over creates a climate of fear that can end up leaving no room for public criticism or dissent. Such environments are not conducive to democracy or social change.

With the reality of a Trump presidency, we should expect an unobstructed furthering of the state's rights in the face of our own.

The **Fourth Amendment** to the U.S. Constitution, alludes to the right to privacy, stating that:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue,

but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[5]

The goal of this provision is to protect people's right to privacy and freedom from arbitrary governmental intrusions. What we currently have in the U.S., is a broken policy framework where the law has failed into protect the rights of certain groups of citizens. Even more drastically, through the frame of "terrorism" the government has an unprecedented ability to surveil anyone who it deems a threat.

If we are really being honest, the right to privacy though has always been for the privileged. Since the U.S. was founded, its government has surveilled, policed, and imprisoned indigenous, black, and other communities of color as part of its policies of state control and to justify its settler colonialism.

From the slave pass, to lantern laws, to predictive policing we have to look at our current mass surveillance state not as an aberration, but rather as the next phase of **a continuing policy of state violence toward our communities.**
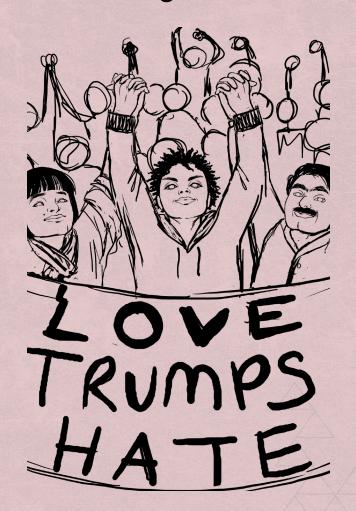
Communities like ours that are in the crosshairs of the current manifestations of mass surveillance must fight even harder for our rights to privacy.

If you are indigenous, black, Muslim, Latinx, undocumented, or LGBTQ you are seen as disposable by the government, your right to privacy has been eroded—or is non-existent. This increases exponentially if you have been part or are curently in the prison industrial complex.

Now, the whole country is experiencing what those of us from these communities have been

saying for a long time:

SHIT IS REAL Y'ALL, and it's time to get to work!

[5] https://www.law.cornell.edu/constitution/fourth_amendment