
Digital Privacy Rights for Immigrants

#StoptheHate Series 11.3.17

Pennsylvania Immigration and Citizenship Coalition





Background

- In late September 2017, The Department of Homeland Security (DHS) announced changes to technology vigilance for all immigrants, including naturalized citizens and possibly any US citizen in communication with someone born or living in another country.
- DHS announced that on Nov. 18 it will begin collecting social media data for all immigrants, including naturalized citizens after a period of public comment.
- It is unclear whether DHS has begun to implement this practice.



What does this mean for immigrants?

- This is another way to intimidate the immigrant community
- Information shared on social media could be used against a person for deportation purposes or to stop a person from getting immigration benefits
- We must know our rights and how to protect ourselves



How ICE Agents Can Use Social Media



- Accuse you of being a gang member because of photos on your account to stop you from getting a green card, DACA, or other legal status
 - For example, DHS can claim a picture of a tattoo, hand signs, or the color of your clothing is gang-related even if is not!
- Investigate or prosecute you for illegal reentry
- Try to put you in “expedited removal,” a special deportation proceeding in which you don’t get to see a judge
- Accuse you of committing a drug crime
- Investigate or prosecute you for using FB, Instagram, YouTube, or public texting to tell others to avoid, run, or hide from a place where an immigration enforcement action such as raid is happening



Web Security Check at the Airport and other Points of Entry





What happens if border agents demand I turn over my device?

- The government claims the authority to search all electronic devices at the border, no matter your legal status in the country or whether they have any reason to suspect that you've committed a crime.
- You can state that you don't consent to such a search, but unfortunately this likely won't prevent CBP from taking your phone.
- If you leave the airport without your device, make sure to get a receipt, which should include information about your device and contact information allowing you to follow up.



Do I have to unlock my device?

Your legal status in the country may inform what you decide to do if you're asked for a password to unlock your device.

Know Your Rights at a Port of Entry

- Can't be denied entry into the country.
- You might be detained for longer or have your device seized and not returned to you for weeks or months.
- Your green card can't be revoked without a hearing before an immigration judge.
- Upon return to the United States, [do not sign a Form I-407 giving up your permanent residence](#), even if an immigration agent pressures you. Ask to speak with an attorney and see a judge.
- If you are not a citizen and are concerned about having your devices searched, you should consult with an immigration lawyer about your particular circumstances before traveling
- If you are a visitor you run the risk of being denied entry if they refuse to provide a password, and they should consider that risk before deciding how to proceed.



Store sensitive data in a secure cloud storage account.

- Disable any connections to cloud-based accounts where you store sensitive communications or files, and don't keep a copy of cloud-stored data in your physical possession
- In July 2017, Customs and Border Protection publicly stated it is against policy for border agents to search cloud-stored data on electronic devices





Turn on airplane mode for all of your electronic devices before crossing a border checkpoint.

- CBP [stated](#) in July 2017 that its policy does not permit searches of cloud-stored data that is accessible from electronic devices through the internet
- Keeping your devices in airplane mode will help ensure compliance with this policy

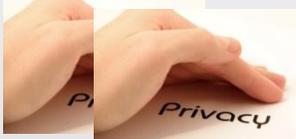


- Disable Touch ID (fingerprint pass codes) when crossing any border
- Save important numbers so you can reach out to family and friends in case your phone or other devices are confiscated.
- Use encrypted text messaging/ video sites
- Turn Off GPS to keep yourself or any community member safe from being tracked



How to protect yourself and your community

Ways to Reduce Risks with Social Media



- Your real name is not necessary
- Do not use your primary e-mail address for your social media accounts
- Change your privacy settings
- **Know your audience**
- Review your profile vs. groups and other people's accounts
- Consider cleaning up or deleting your Facebook or other social media accounts
- Turn off location on social media
- Set up privacy settings for pictures, videos, post, etc



Digital Security in the Age of Trump

- **Equality Labs- Digital Security in the Age of Trump: Self-Defense Curriculum** - <https://www.equalitylabs.org>
- **ACLU: Your Rights at Airports and Other Points of Entry** - <https://www.aclu.org/know-your-rights/what-do-when-encountering-law-enforcement-airports-and-other-ports-entry-us>
- **Can Border Agents Search Your Electronic Devices? It's Complicated-**
<https://www.aclu.org/blog/privacy-technology/privacy-borders-and-checkpoints/can-border-agents-search-your-electronic?redirect=blog/free-future/can-border-agents-search-your-electronic-devices-its-complicated>
- **National Immigration Project of the National Lawyers Guild: Social Media, Criminalization, and Immigration-**https://www.nationalimmigrationproject.org/PDFs/community/2017_03Apr_comm-adv-social.pdf
- **Surveillance Self-Defense** - <https://ssd.eff.org/en/playlist/want-security-starter-pack>
- **The Rights of Lawful Permanent Residents, March 2017-**
https://www.ilrc.org/sites/default/files/resources/lpr_info_sheet_final_march_2017.pdf

New Tactics?

ICE Agents Are Starting to Text Immigrant Targets

They're Also Continuing Constitution-Violating Arrests





Do's & Don'ts

- Don't call out and tag undocumented immigrants on social media
- Be careful about when you tag people
- Don't share people's phone numbers, e-mails, or addresses online without their permission
- Make your account private and only accept request from people you know