Will the Department of Homeland Security (DHS), or other federal agencies outside of the Census Bureau, have access to individual response data in the event of a data breach?

Although DHS and other security experts are helping with the Census Bureau, in the event of a data breach, they will only have access to IP addresses and limited metadata.

What are the best browsers to use when responding online?

The best options for responding online will be to use the latest version of Internet Explorer, Safari, Chrome, or Firefox. The Census Bureau is testing the Internet Self Response (ISR) in the current and prior year versions of these browsers.

What devices are best for responding online?

Desktop PCs, iPhone versions 5 and later, most iPad versions, and Samsung Galaxy phones and tablets.

If we do have kiosks or other digital access points, what are best practices for securing kiosks?

The Census Counts campaign has a comprehensive guide on best practices for securing kiosks, which you can find here.

II. Misinformation & Disinformation

Identifying Census Disinformation

The lead-up to the census has produced large quantities of information and commentary about the upcoming count, which are circulating via news channels, social media, and other networks. However, not all available information on the 2020 Census is factual. Given the sheer volume of information that is created and shared each day, spotting inaccurate information can pose an ongoing challenge. Based on the work of the research institute Data & Society, below is an outline of simple strategies your city can follow to identify and mitigate information threats. Furthermore, while these skills are critical for the census, they will also serve city leadership well in a multitude of situations, ranging from emergency response to elections.

What is Disinformation and Why Does It Matter?

Obtaining a fair, representative, and accurate 2020 census count is vitally important. Political representation, access to funding, and distribution of public resources in your city all depend on your constituents’ decision to fill out the census. Minimizing disinformation helps to create a society in which everyone counts.

Your constituents make decisions based on information from a variety of sources. While census information shared through government channels is likely to be verified, constituents will receive and trust information from other sources such as friends, family members, or social media accounts. This information may be partially or entirely fabricated depending on the biases, fears, beliefs, and motives of the person who shared it. Two types of factually inaccurate content exist. The first, misinformation, refers to false claims spread by individuals or organizations
with good intentions who believe those claims to be true. For example, if an ill-informed individual shared with her Twitter followers that the 2020 census could only be filled out online, this would be considered misinformation.

The second type, disinformation, refers to false claims spread intentionally to cause harm. In the case of the census, bad actors may spread disinformation with the objective of suppressing participation in, or otherwise manipulating behavior around, the decennial count. Disinformation may be created as propaganda, to push a political agenda, or as part of a scam. For example, if a Twitter account mimicked the branding of a legitimate news outlet to spread false information and deceive readers, this would be considered disinformation. Disinformation may be part of a disinformation campaign, or a coordinated effort between multiple actors to influence people through false or misleading content. Both misinformation and disinformation may inhibit census participation if not checked, though it is hard to know in advance how much of a role this will play in 2020. This resource will focus primarily on disinformation, as it is more difficult to stop.

What Does Disinformation Look Like?

While disinformation can take many forms, in the case of the census, any content, hashtags, images, or videos that may suppress census participation should be investigated further for signs of manipulative or inauthentic behavior. For example, if a community of Twitter users in your city begin tweeting about a census boycott using a specific hashtag, you may wish to use the techniques in this guide to explore the origins of the hashtag to assess whether a coordinated disinformation campaign may be behind it. In addition, while not always signs of disinformation, traits like heavy bias, lack of professionalism, poor writing, overly emotional language, mimicry of legitimate news sources, and embellishment may indicate that an article or post is worth further exploration for signs of disinformation.

In addition, bad actors may edit photos and videos or use them out of context to support a disinformation agenda. Since photos are easy to edit, always question images that purport to show controversial or potentially incendiary content. Bots, or computer programs designed to auto-generate and interact with social media posts, may also be used to spread disinformation and fabricate the appearance of support for a viewpoint or agenda. Remember: disinformation is not be limited to public online channels — it may be spread through closed networks (such as private WhatsApp or Facebook messaging groups), real-world communities (such as social or religious groups that meet in person), or through traditional media channels.

While separating disinformation from factual sources can be challenging, there are steps your city can take to prevent, prepare for, and respond to disinformation and keep it from gaining traction.

What Can My City Do?

Prevention | It’s difficult to know if, where, and when disinformation will appear. However, there are proactive steps your city can take to identify potential sources of disinformation and create an atmosphere that counters disinformation from spreading.

- Monitoring | Ask partners and collaborators to regularly share the details of websites, social media accounts, or other sources that are suspected of spreading false information around the census. Keep tabs on the veracity of information that these actors are spreading. Technologies like Hootsuite and Google Alerts can be used to easily track local mentions of the census and monitor potentially problematic hashtags on social media. If disinformation is discovered but online traction and engagement is low, avoid responding so that you do not inadvertently spread the disinformation further.

- Identify Adversarial Amplifiers and Trusted Messengers | Identify key actors and organizations that are likely to amplify disinformation and monitor them closely including social media accounts with outsized
influence. Similarly, identify actors and organizations that your constituents trust and build working relationships with them. Raise awareness about disinformation among these trusted messengers so that they can be mobilized to counter a future disinformation campaign.

- **Fill Data Voids** | Ensure that correct and accurate census information is available and easily searchable for constituents. In cases where little factual content exists on the internet, bad actors may co-opt common search terms so that disinformation rises to the top of search queries. Moreover, since the census only happens once per decade, “census” itself is a data void, as relatively little legitimate online content has been created for the census. As a result, false or misleading census content rises to the top of search results more quickly. To combat this, put all of your city’s census content online and optimize your content for search engine discovery in response to census queries. Coordinate messaging with local partners and stakeholders to ensure messaging is clear and not conflicting. The larger and more accessible your repository of factual content, the harder it will be for disinformation agents and media manipulators to find a data void to exploit.

- **Understand Social Media Platform Policies on Disinformation** | Twitter, Facebook, YouTube, and other social media platforms have policies that govern what constitutes disinformation and how the platform will react to it. Locate and read these policies for platforms you use regularly and review how to flag or report disinformation and misleading accounts on each platform. Disinformation policies and reporting guidelines for major social media platforms are included in the Additional Resources section.

**Preparation** | Consider the steps that your city will follow if a disinformation campaign arises. Being prepared helps you to act appropriately and decisively if a problematic narrative begins to spread.

- **Create Inoculation Messages** | Develop messaging that “inoculates” your constituents against believing disinformation. Inoculation messaging primes your audience to be on the lookout for false claims by explaining why bad actors may be spreading disinformation while simultaneously repeating and amplifying the truth.

  **Sample Inoculation Message:** “Anti-immigrant groups are discouraging noncitizens from taking the census. Anyone who is urging you not to fill out the census is actually trying to suppress the count and deprive certain communities of funding and representation. The census counts everyone living in the United States – no matter what their citizenship status might be – and census data is used to provide crucial funding and representation for ALL communities. Everyone should fill out the census as completely as they can.”
  
  Source: Data & Society

- **Minimize Amplification of Disinformation** | Calling attention to false narratives, even in an effort to denounce them, may inadvertently spread the disinformation further. If online traction and engagement is low, nonresponse to disinformation is usually the best policy. If a response is required, limiting refutation of disinformation to the original channels used to promote it helps to keep the false narrative contained.

  **To Refute or Not to Refute?**

  Paradoxically, responding to disinformation, even to refute it, can give the disinformation oxygen and allow it to spread and flourish. If few people have seen the disinformation in the first place, publishing a
public refutation may actually amplify the disinformation to a wider audience. In cases where the original audience is small and the false information is not spreading or jumping to new channels, it is best to ignore disinformation and not respond or refute it.

In cases where the number of people exposed to the disinformation is beginning to grow, it may make sense to refute the disinformation in a restrained, limited fashion. For example, let’s say that a problematic narrative is circulating through a popular closed Whatsapp group chat. Members of the chat have seen the disinformation, but it has not yet spread to public social media platforms. However, you are concerned that group members are forwarding the disinformation via private messages to family and friends who are likely to believe and act on it. In this case, you could have a trusted messenger directly refute the disinformation within the Whatsapp group. However, it would be inadvisable to publish a broad response to the disinformation on other platforms, because in doing so, you could inadvertently amplify the disinformation among populations who have not yet encountered it.

It is often challenging to recognize the “tipping point” that determines whether or not a response is warranted. To do so, you may ask the following questions to estimate whether the narrative is spreading:

- Has the problematic content shifted from insular, discrete communities to a wider audience?
- Has the disinformation jumped from one platform to another?
- Has online engagement with the problematic post or narrative surpassed a specific threshold (for example, has social media interaction reached four digits)?
- Has the disinformation reached or been spread by influential amplifiers?

If you answered “yes” to several of the above questions, you might consider whether it makes sense to refute the disinformation in a restrained fashion. However, ultimately your city should carefully consider the potential positive and negative effects of refuting a particular problematic narrative. Ensure that the pros outweigh the cons before issuing a response.

- **Practice Rapid Response |** Anticipating possible disinformation scenarios that may arise and considering how your city might respond to them will help ensure coordinated, rapid action should disinformation emerge.

**What Would We Do If...?**

To date, it is uncertain whether disinformation will pose a major threat to the 2020 Census. However, it is a good idea for cities to plan ahead and consider how they would respond to different types of disinformation threats before disinformation becomes a problem. This will help ensure that your staff keeps calm and acts in a coordinated and strategic manner if a threat emerges. Remember, sometimes the best response is no response at all.

How would you react to the following scenarios? What other scenarios may occur in your city that you should prepare for?

- News is circulating that census enumerator devices have been hacked. Reporters remark that
they have seen data that looks like census data and the Commerce Department says that it is investigating. This may be a hoax or it may be real. Your community is beginning to panic. What do you do?

- A photo is circulating on WeChat in your city depicting an Asian man in handcuffs at his front door with an ICE officer, with a message in Mandarin saying “Don’t answer the door. It’s ICE, not the Census Bureau.” What do you do?
- While reading through your city’s main daily newspaper, you notice that a major news story was published this morning discussing the likelihood of a hacker gaining access to the U.S. Census Bureau database. While the facts presented in the story are correct, the narrative seems to substantially overstate the likelihood that a breach will occur. Later that day, you see the same article being shared multiple times on Facebook with concerned comments. What do you do?

Source: Data & Society

Response | When disinformation emerges, city governments are often a first point of contact for constituents. Responding appropriately and decisively to disinformation is vital to containing the threat.

- **Verify Veracity of Problematic Information** | Determine whether suspected disinformation is factual or not. Keep in mind that even content with factual origins may be misrepresented or altered to promote a false narrative. The techniques in the Tools and Resources box can assist you in determining the veracity of problematic content.

- **Identify Disinformation Techniques** | Identify whether a specific disinformation technique is in use. While media manipulators are creative and resourceful, their tactics may follow recognizable patterns. Identification of these patterns can help your city predict how the false narrative will spread and you can craft an appropriate response.

  - **Sockpuppetry** | This technique involves either human or bot “sock puppets” pretending to be something they are not online.
    - **For example:** A social media bot may falsely pose as a local immigrant rights activist and post content discouraging census participation in immigrant populations.
    - **Possible response:** Use the tools and resources below to assess whether the account is real. If not, report the fake account to the relevant social media platform for removal.

  - **Keyword Squatting** | This technique involves media manipulators filling data voids with false or misleading content designed to be keyword searchable and rise to the top of search engine results.
    - **For example:** Taking advantage of a lack of census content on the internet, a bad actor generates a large quantity of misleading content full of census keywords so that search engines return the misleading articles when someone searches “Census 2020”.
    - **Possible response:** Creation of genuine census content to fill data voids and search engine optimization to ensure that search engines return accurate content.

  - **Controlled Opposition** | This technique involves sock puppets (either bot or human) seeking to disrupt a particular online community by posing as community members and spreading false narratives.
For example: A bad actor posing as a renter may spread false rumors in an online affordable housing forum that accurately filling out the census can lead to eviction.

Possible response: Use the tools and resources below to assess whether the account is real. If not, report the fake account to the forum administrators for removal.

Apply Threat Classification and Implement Response | Using the threat classification framework that your city developed, determine the severity of the disinformation threat and decide upon an appropriate response.

Tools and Resources

Detect Edited Images | Media manipulators may edit photos or videos in misleading ways or may use images out of context to promote a false narrative.
  ○ Google reverse image search allows you to search the internet for similar images and detect whether media manipulators have edited an existing image to support their narrative.
  ○ FotoForensics is a tool that analyzes images for signs of manipulation by editing software.
  ○ InVID is a browser plug-in that detects traces of video editing and finds original web sources for videos.
  ○ SurfSafe is a browser extension for Google Chrome, Firefox, and Opera that identifies original image sources.

Identify Bots and Fake Accounts | Bots and fake social media accounts are used to promote false narratives and grant the illusion of credibility to a disinformation campaign. While the below methods can help to identify fake accounts, they are not foolproof. However, if an account is flagged by several bot detection tools, it may indicate possible suspicious activity that should be evaluated further.
  ○ Look at social media platform metadata to assess whether a problematic account is a bot. For example, you can easily download Twitter records in spreadsheet format to check for rapid successions of tweets from different locations, which is one sign of possible bot activity. For more information on how to read social media metadata, view this infographic from Data & Society.
  ○ Search for the same username on other social media platforms to assess whether the account appears to be a real person. You can also search the timestamps of posts to help verify whether the account is a bot, as any human user will take regular breaks from posting (to sleep, for example).
  ○ Search for the account using the Wayback Machine, an internet archive that stores historical snapshots of websites, to see if an account’s followers have grown at a normal rate over time.
  ○ Botcheck.me is a browser plug-in that rates each Twitter user profile with how confident it is that the user is a bot account. Download here.
  ○ Botometer is a web tool that uses Twitter activity history to estimate the likelihood that an account is a bot. Access the tool here.

Track Problematic Narratives | Set up alerts so that you receive early notification when disinformation emerges.
  ○ Set Google alerts for census keywords in your city to receive a daily email digest summarizing the keywords’ use in online media. This tactic can be a useful way to monitor for problematic news items. Follow these steps to set up a Google alert. Potential alert keywords may include
“census”, “<city name> + census”, “census + immigrant”, or specific keywords or hashtags linked to problematic narratives you have observed.

- Use Hootsuite or similar social media management tools to follow the conversation around hashtags related to the 2020 Census and identify upticks in usage of problematic hashtags.

## Additional Resources

- The Yalla Count Me In campaign at the Arab American Institute has developed a wealth of shareable educational resources on census disinformation.

- First Draft News has developed an informative series of training videos on topics ranging from information verification to identifying photo manipulation and using Google Reverse Image Search.

- The Leadership Conference’s Census Counts Campaign has released a GOTC toolkit containing helpful resources on how to manage disinformation threats.

- The Census Bureau maintains a “rumors” webpage that tracks false information circulating around the census and sets the record straight.

- Color of Change maintains a portal where people can report false census rumors they encounter.

- NALEO maintains a toll-free, bilingual census hotline (877-EL-CENSO or 877-352-3676) to provide free census information that is geared toward Latinx communities but is available to everyone.

- For an in-depth exploration of how to use social media metadata to identify media manipulators, read Dr. Amelia Acker’s report: Data Craft: The Manipulation of Social Media Metadata, published by Data & Society.

### III. Digital Divide & Access

**What is the Digital Divide?**

In 2020, for the first time in the history of the U.S. census, respondents will be able to fill out their census forms online. While the digital option may be a convenience for many, it also makes it more likely that people with low internet proficiency or access may be excluded. Communities with low internet connectivity and low levels of digital literacy may be especially vulnerable to an undercount. According to the Federal Communications Commission (FCC), approximately 24 million Americans live without access to broadband internet. Only about 75% of rural Americans and 68% of those living on tribal lands have broadband access. Racial disparities in broadband access also persist — in 2018, approximately half of African American and Hispanic adults reported they had home broadband access, compared to 72% of white adults. While broadband coverage is lowest on average in rural, Western states, internet deserts also exist in cities, especially among poorer, older, less educated populations. The digital divide, therefore, refers to two separate but related problems: a lack of internet connectivity at home and a lack of digital literacy. Some people may be affected by both issues, while for others only one of the above

---
