Final Project Submission

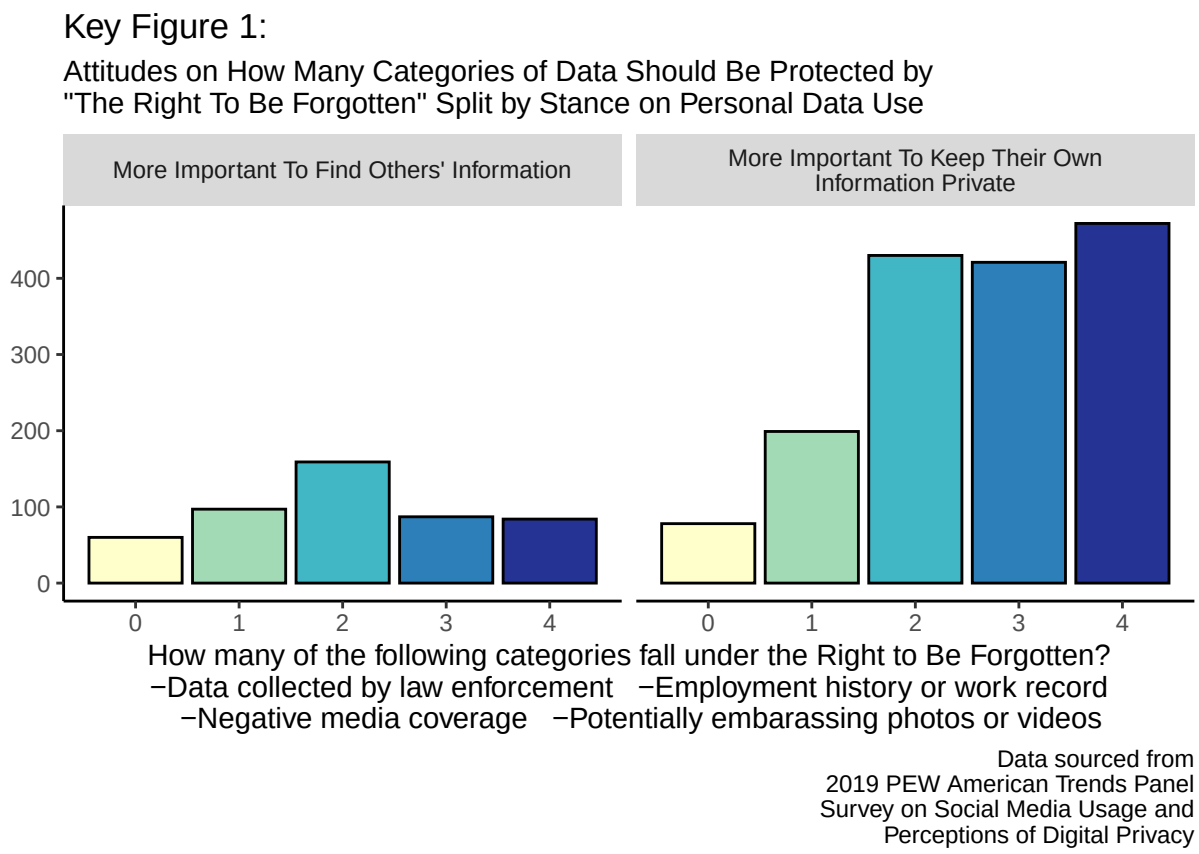
Jake Chanenson and Adriana Knight

5/12/2021

Introduction

Our physical and digital lives have been increasingly entwined during the first two decades of the twenty first century as we enter into the digital age. A direct consequence of this development is the advent of what social psychologist Shoshana Zuboff calls "Surveillance Capitalism" – an economic model where a user's personal data is commodified for profit generation. The commodification of personal data comes at the cost of user privacy as companies hoover up any and all quantifiable metrics about a given user in an effort to serve them more ads and services that are tailored to them (Buttarelli, 2018) (Zuboff, 2019). As such, it is now more important than ever to understand how the American people feel about issues surrounding the use of their data and their privacy. We chose two aspects of digital privacy to focus on: public sentiment surrounding the Right to Be Forgotten (RTBF) – a privilege for people to remove photos, documents, and videos of themselves from public internet search – and the privacy threat of Facial Recognition Technologies.

Key Figure 1



Explanation of Key Figure 1

In May 2014, almost seven years ago exactly, the European Union instituted a rule wherein individuals could request for links pointing to sensitive information about them to be expunged from search engines, on grounds of inadequacy, irrelevance, or excess (Chenou, J.-M., & Radu, R., 2019). This new ruling is imperfect, and grounds for controversy. Namely, the institution of private near-monopolistic tech companies as quasi-governmental arbiters of digital rights is a source of extreme concern. Critics point to the foundation of these companies' business models on the collection of data which the ruling would try to protect as a conflict of interest that poses dangerous concern. Put another way, "the information age is based on productivity of knowledge. Information constitutes society's raw material" (Seubert, S., & Becker, C. 2019). The "raw material" of information, as some may describe it, is filtered and folded into larger and more complicated digital profiles that may be used productively. "As so much is tracked and measured, it can be monetized and marketized and subjected to the larger forces of financial capitalism" (Silverman, J., 2017). The Right to Be Forgotten, for some, may feel like a radical shift, and for others may feel like a reinforcement of the status quo of surveillance capitalism, dressed up in a falsely compassionate guise. But what is the Right to Be Forgotten, on a practical level? How do ordinary people – not tech conglomerates or social scientists – grapple with their own and others' data in an increasingly digitized world? The above visualization aims to unpack at least a small portion of that, taking aim on where the public's priorities lie and how respondents may view their and others' information in relation to the public sphere.

The primary question we had when approaching the data set was what people conceive of (within their personal data) as private, versus what they view as something that falls within the purview of public discourse. In other words: what information about themselves do people think exists within the public domain, and what information about themselves should be protected? The wide range of new information technologies that have sprung into being in the last few decades redefine and complicate our previous understandings of the public versus private spheres; developments in technology have increased the capacity to access, store, and share information about personal matters. Though, our understanding of these boundaries remains in flux, and what cannot be described, defined, and understood cannot be defended or regulated (Bajpai, K., & Weber, K., 2017). As such, the first step to enact any sort of policy or engage in any public discourse is to first gauge public opinion.

There are two questions relating to this topic in the survey our data set is sourced from: one is general (`PUBLICDATA_W49`, which asks respondents to identify whether it is more important to have access to everyone's data or to keep their own data private) and one is specific (`RTBF_a`, `RTBF_b`, `RTBF_c`, `RTBF_d`, each of which ask respondents to choose whether an identified category of personal data should exist within the public or private spheres). We were interested in exploring how these two sets of questions interface with one another, and any trends we could find between responses.

Of participants who responded to the public data question, the vast majority (about 75%) of respondents responded saying that they found it to be more important to protect one's own personal data than to have access to others'. This trend was reflected across the board for all responses to questions examining the Right to Be Forgotten as applied to specific categories of data. What we found to be much more interesting in our exploration was examining internally, between the two categories (public-data driven respondents and private-data driven respondents) to see what the distribution of protected data types turned out to be. We created a dummy variable which counted how many categories of data a given participant identified as being protected, and for each category of respondent mapped out the distribution of these sum counts.

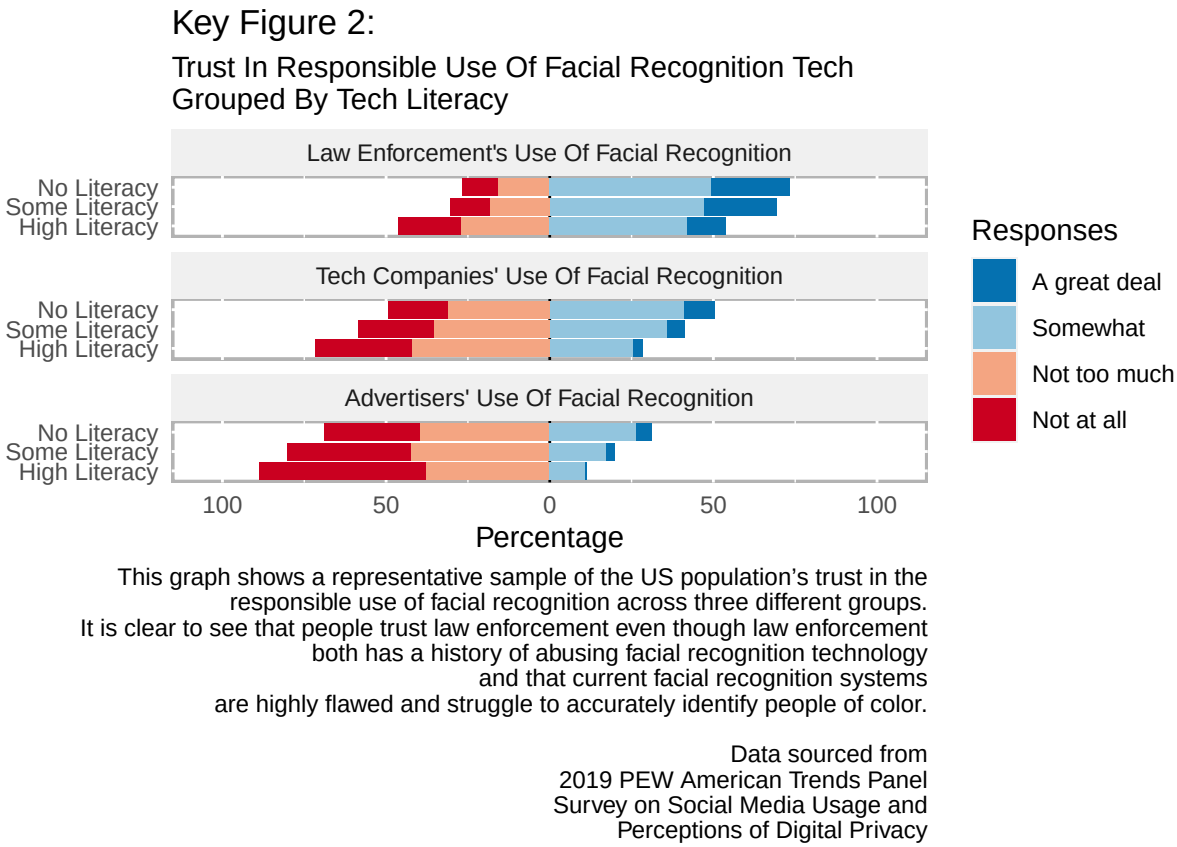
The final visualization we selected shows these two distributions of visualizations side by side, to show both the difference in scale as well as the difference in internal distributions between the two. Immediately it becomes apparent, looking at key figure 1, that the distributions are different between these two categories of people; of those who are public data driven, the distribution of counts is approximately normal, peaking at two out of four categories of data being protected. For those respondents who are private data driven, the distribution of counts is left skewed, with the majority of respondents preferring higher numbers, if not all four, of the identified categories of data falling under the right to be forgotten.

It was also important to us that the visualization register the scale of counts of responses. As mentioned before, the majority of respondents identified maintaining their own private data as being more important/valuable

to them than having access to others'. We elected not to normalize the scale between these two categories, as not only does the distribution of protected category counts show something about the respondents' opinions, so does the sheer scale by which these categories differ.

The resulting image allows the viewer a glimpse into the two major camps as identified by the survey, but does not reduce them to a simple binary, instead showing more intriguing trends in conceptualization of what is or isn't private. It shows both internal distributions but also how different these two groupings of public or private data driven people are in their perceptions of what is or isn't worth protecting.

Key Figure 2



Explanation of Key Figure 2

Current facial recognition systems are far from accurate and are plagued with issues of bias in their datasets (Buolamwini & Gebru, 2018). These systems are built to search for a match in hundreds of thousands of faces extremely quickly (Venema, 2020), however, they are trained to recognize primarily white, cisgender male faces – meaning that they perform poorly on everyone else. Indeed, to highlight this issue, the ACLU ran the faces of the 115th United States Congress through Amazon's off the shelf facial recognition tool called "Rekognition." Amazon Rekognition identified 28 members of Congress as "other people who have been arrested for a crime." Of those false matches "40 percent... were of people of color, even though they make up only 20 percent of Congress" (Snow, 2018).

In short, facial recognition in the early 21st century is a highly flawed tool that outputs racist results and is a threat to the privacy of the general public. Currently, there is no national regulation of facial recognition technology (Crawford, 2019). However, public opinion of facial recognition technology can shape policy which can lead to privacy protections. It is therefore vitally important to understand how public opinion differs for various groups using facial recognition technology.

Rather than just display the preexisting results from the Likert scale in the Pew survey, we decided to partition the data based off of how knowledgeable the respondent was about technology; in other words, we quantified their tech literacy. An in-depth explanation about how and why this tech literacy variable was created can be found with the accompanying explanation of additional figure 1 for key figure 2.

Turning our attention back to the figure, within each facet there is a clear correlation between level of tech literacy and distrust of a given group using facial recognition technology responsibly. Moreover, there is a clear ranking across the facets, regardless of tech literacy level, which trusts law enforcement to responsibly use facial recognition technology the most, tech companies the second most, and advertisers the least.

The literacy-distrust correlation within each facet makes sense because those who know more about technology may be more aware of potential issues and pitfalls around facial recognition. Indeed, the converse is also true. Those who have no tech literacy likely have no technological domain knowledge and, as such, may at best have a superficial understanding of facial recognition.

The ranking preference across the facets, however, is concerning. Many experts call for a ban of facial recognition use (Bennett, 2011) (Crawford, 2019) because they do not trust that the technology can be used responsibly by any party. This does not line up with public opinion. From a perspective of a trust-distrust dichotomy, key figure 2 indicates that a majority of respondents only have an overwhelming distrust of advertisers. In addition, the respondents on the whole have more distrust than trust for tech companies to use facial recognition responsibly with the respondents with no tech literacy dead even with 50% trust and 50% distrust. The most concerning finding here, however, is that the majority of respondents, regardless of literacy level, trust law enforcement to use facial recognition responsibly. This is very concerning as law enforcement both has a history of abusing facial recognition technology (Devich-Cyril, 2020) and that, as mentioned above, current facial recognition systems are highly flawed and struggle to accurately identify people of color. This glut of trust for law enforcement – especially as compared to the dearth of trust for advertisers – could indicate a relative unwillingness to regulate law enforcement's use of facial recognition technology. One possible explanation for the difference between expert opinion and public sentiment is that the respondents of the survey have a poor understanding of the limitations of facial recognition technology as seen in Additional figure 3 for key figure 2. They believe accurately identify people, assess gender, and assess race. They are incorrect (Buolamwini & Gebru, 2018) (Crawford, 2019).

Bibliography

Bajpai, K., & Weber, K. (2017). Privacy in Public: Translating the Category of Privacy to the Digital Age. In *From Categories to Categorization: Studies in Sociology, Organizations and Strategy at the Crossroads* (Vol. 51, pp. 223–258). Emerald Publishing Limited. https://doi.org/10.1108/S0733-558X20170000051006

Bennett, C. J. (2011). In further defence of privacy… *Surveillance & Society*, *8*(4), 513–516. http://dx.doi.org/10.24908/ss.v8i4.4189

Buolamwini, J., & Gebru, T. (2018). *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. 15. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Buttarelli, G. (2018). Big Tech Is Still Violating Your Privacy. *New Perspectives Quarterly*, *35*(4), 13–16. https://doi.org/10.1111/npqu.12169

Chenou, J.-M., & Radu, R. (2019). The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union. *Business & Society*, *58*(1), 74–102. https://doi.org/10.1177/0007650317717720

Crawford, K. (2019). Halt the use of facial-recognition technology until it is regulated. *Nature*, *572*(7771), 565–565. https://doi.org/10.1038/d41586-019-02514-7

Devich-Cyril, M. (2020, July 5). *Defund Facial Recognition*. The Atlantic. https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/

Seubert, S., & Becker, C. (2019). The culture industry revisited: Sociophilosophical reflections on 'privacy' in the digital age. *Philosophy & Social Criticism*, *45*(8), 930–947. https://doi.org/10.1177/0191453719849719

Silverman, J. (2017). Privacy under Surveillance Capitalism. *Social Research*, *84*(1), 147–164.

Snow, J. (2018, July 26). *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*. American Civil Liberties Union. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (First edition). PublicAffairs.

Appdendix

Description of Dataset

The dataset we used is the 2019 PEW Survey on American Trends on Technology. The full citation for this data set is as follows:

Pew Research Center. (2019). American Trends Panel (W49). Retrieved from https://www.dropbox.com/sh/adyrtaju2jd7a2d/AAC2fmHoYs2SwVYKqCIkTxOsa?dl=0

The data set is a sample of 4272 respondents of people 18 years or older living in the US. This sample consisted of both English and Spanish-language survey takers. The methodology also details the stratified sampling. I have copied the statement from the methodology section below:

> The ATP subsample was selected by grouping panelists into seven stratum 1. Non-internet panelists. There were 691 total panelists in this stratum and they are sampled at a rate of 100% 2. HS or less panelists. There were 2,027 total panelists in this stratum and they are sampled at a rate of 98.9%. 2,005 panelists were selected for Wave 49. 3. Hispanic, Unregistered or Non-volunteers. There were 5,312 total panelists in this stratum and they are sampled at a rate of 44.8%. 2,380 panelists were selected for Wave 49. 4. Black or 18-34 panelists. There were 1,253 total panelists and they are sampled at a rate of 18.2%. 228 panelists were selected for Wave 49. 5. Other panelists. There were 4,176 total panelists and they are sampled at a rate of 13.5%. 564 panelists were selected for Wave 49.

Variables Used and Their Questions Phrasing Key Figure 1

- `PUBLICDATA_W49` - "Today a wide range of information about people is searchable online. Do you think it is more important for people to have the ability to. . . "
- `RTBF` - "Do you think that ALL Americans should have the right to have the following information about themselves removed from public online search results?"
  - `RTBFa_W49` - "Data collected by law enforcement, such as criminal records or mugshots"
  - `RTBFb_W49` - "Information about their employment history or work record"
  - `RTBFc_W49` - "Negative media coverage"
  - `RTBFd_W49` - "Potentially embarrassing photos or videos"

Key Figure 2

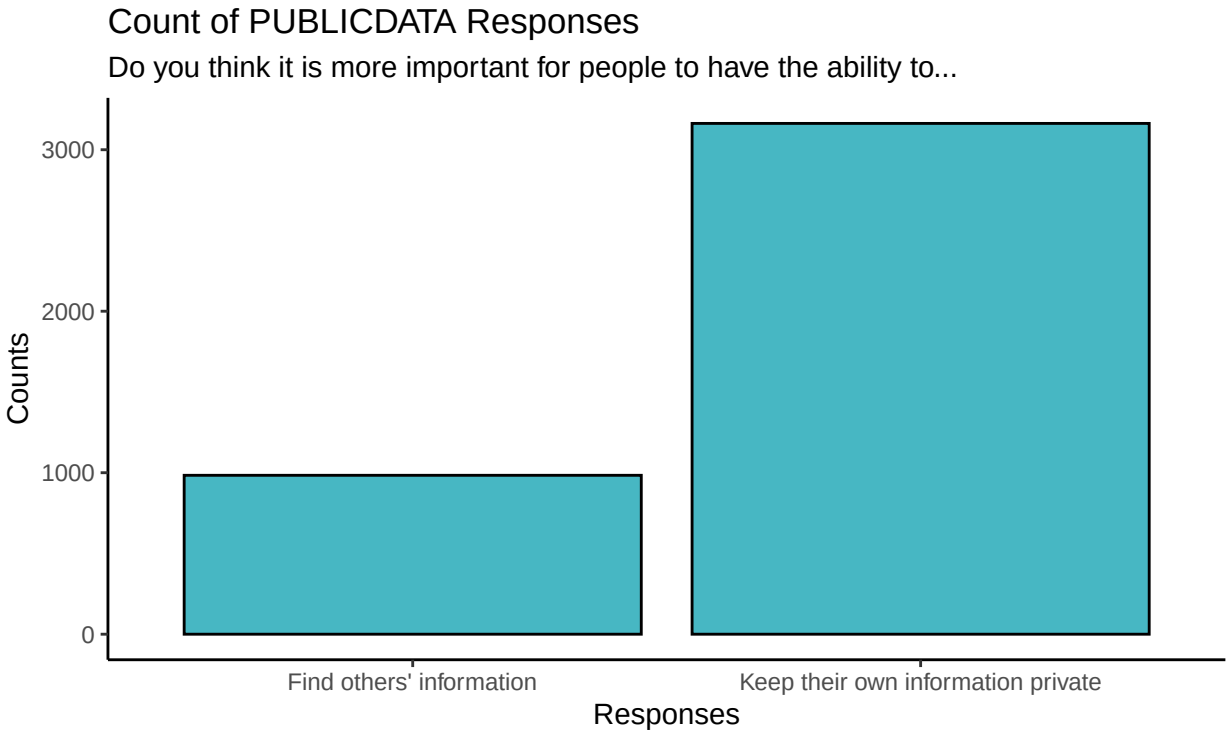
- `FACE1` - "How much have you heard or read about the development of automated facial recognition technology that can identify someone based on a picture or video that includes their face?
- `FACE2` - "Based on what you know, how effective do you think facial recognition technology is at the following things?"
  - `FACE2a_W49` - "Accurately identifying individual people"
  - `FACE2b_W49` - "Accurately assessing someone's gender"
  - `FACE2c_W49` - "Accurately assessing someone's race"
- `FACE3` - "How much, if at all, do you trust the following groups to use facial recognition technology responsibly?"
  - `FACE3a_W49` - "Advertisers"
  - `FACE3b_W49` - "Technology companies"
  - `FACE3c_W49` - "Law enforcement agencies"
- `FACE4` - "In your opinion, is it acceptable or unacceptable to use facial recognition technology in the following situations?"

  - FACE4a_W49 - “Law enforcement agencies assessing potential security threats in public spaces”
  - FACE4b_W49 - “Companies automatically tracking the attendance of their employees”
  - FACE4c_W49 - “Advertisers seeing how people respond to public advertising displays”
  - FACE4d_W49 - “Apartment building landlords tracking who enters or leaves their buildings”
- KNOW1_W49 - "If a website uses cookies, it means that the site...
- KNOW3_W49 - “When a website has a privacy policy, it means that the site...”
- KNOW4_W49 - “What does it mean when a website has ‘https://’ at the beginning of its URL, as opposed to ‘http://’ without the ‘s’?”
- KNOW7_W49 - “The term ‘net neutrality’ describes the principle that...”
- KNOW8_W49 - “Many web browsers offer a feature known as ‘private browsing’ or ‘incognito mode.’ If someone opens a webpage on their computer at work using incognito mode, which of the following groups will NOT be able to see their online activities?”
- KNOW9_W49 - “Some websites and online services use a security process known as two-step or two-factor authentication. Which of the following images is an example of two-factor authentication?”
- CONCERNCO_W49 - “How concerned are you, if at all, about how companies are using the data they collect about you?”

Additional Figures For Key Figure 1

1. Count Of PUBLICDATA Responses

```
## Warning: Vectorized input to `element_text()` is not officially supported.
## Results may be unexpected or may change in future versions of ggplot2.
```

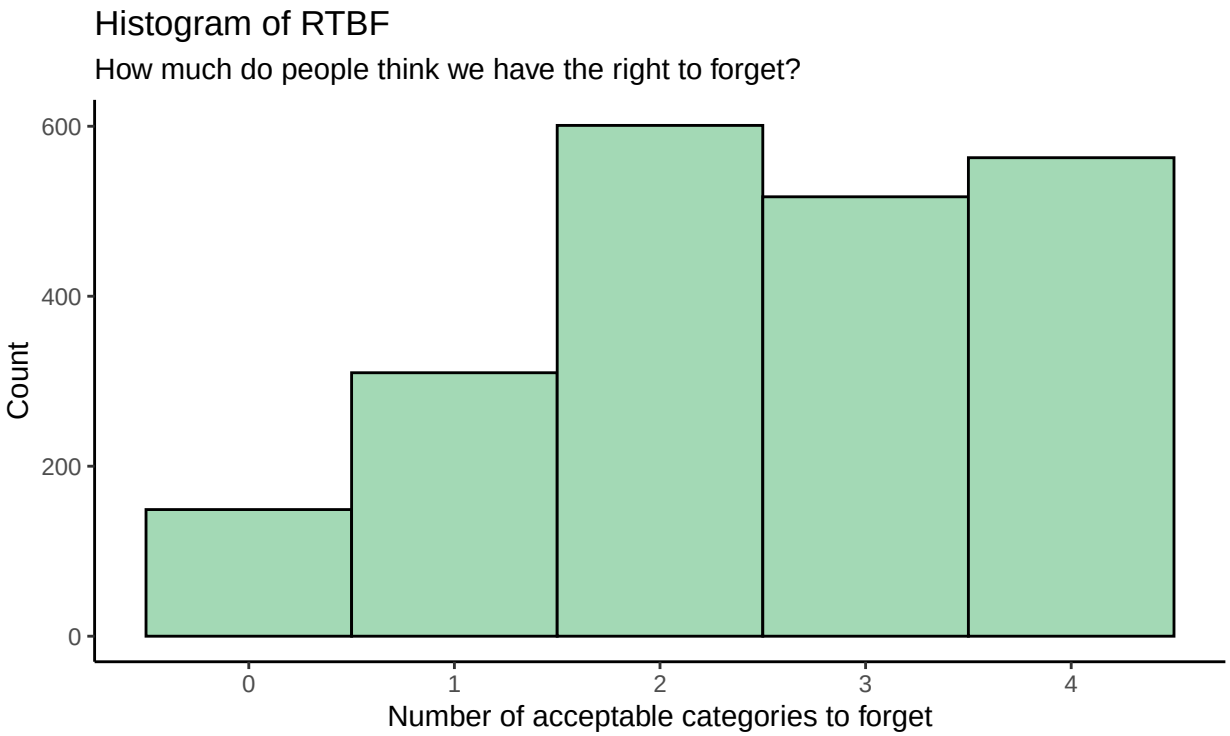


Additional Figure 1
For Key Figure 1

Data sourced from
2019 PEW American Trends Panel
Survey on Social Media Usage and
Perceptions of Digital Privacy

2. How Much Data Do People Think We Have The Right To Forget

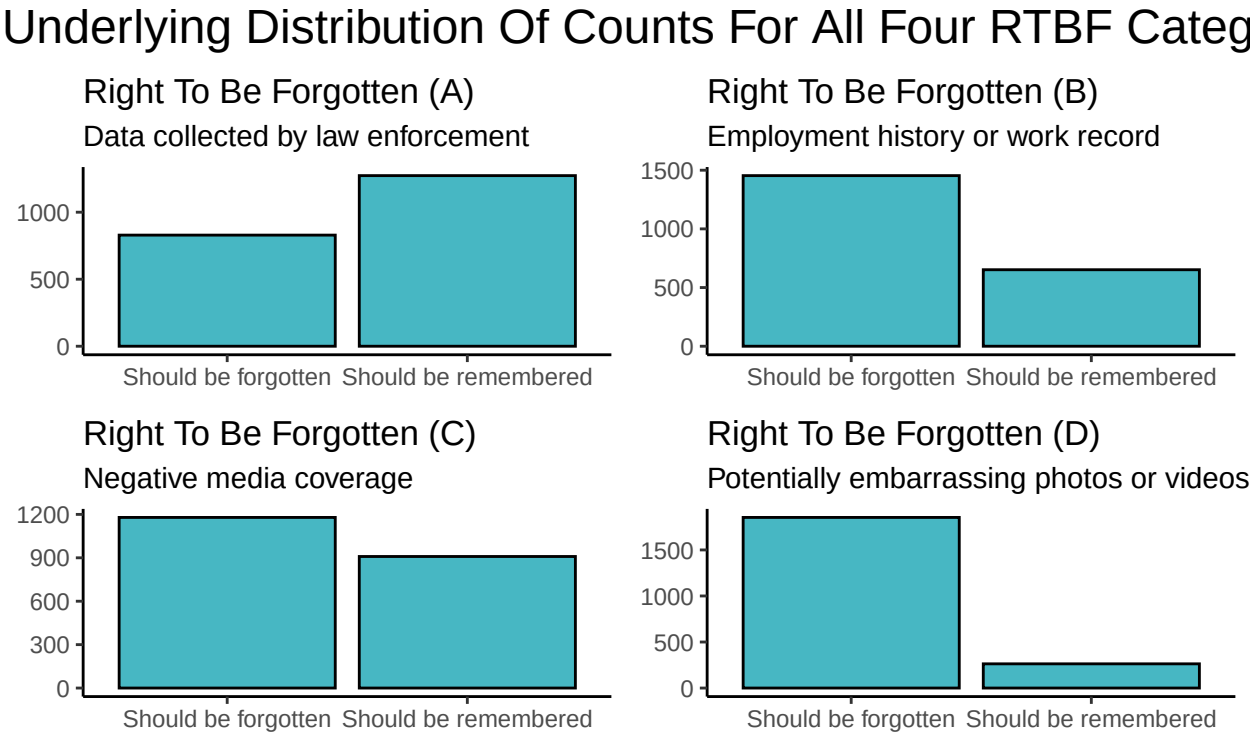
```
## Warning: Vectorized input to `element_text()` is not officially supported.
## Results may be unexpected or may change in future versions of ggplot2.
```



Additional Figure 2
For Key Figure 1

Data sourced from
2019 PEW American Trends Panel
Survey on Social Media Usage and
Perceptions of Digital Privacy

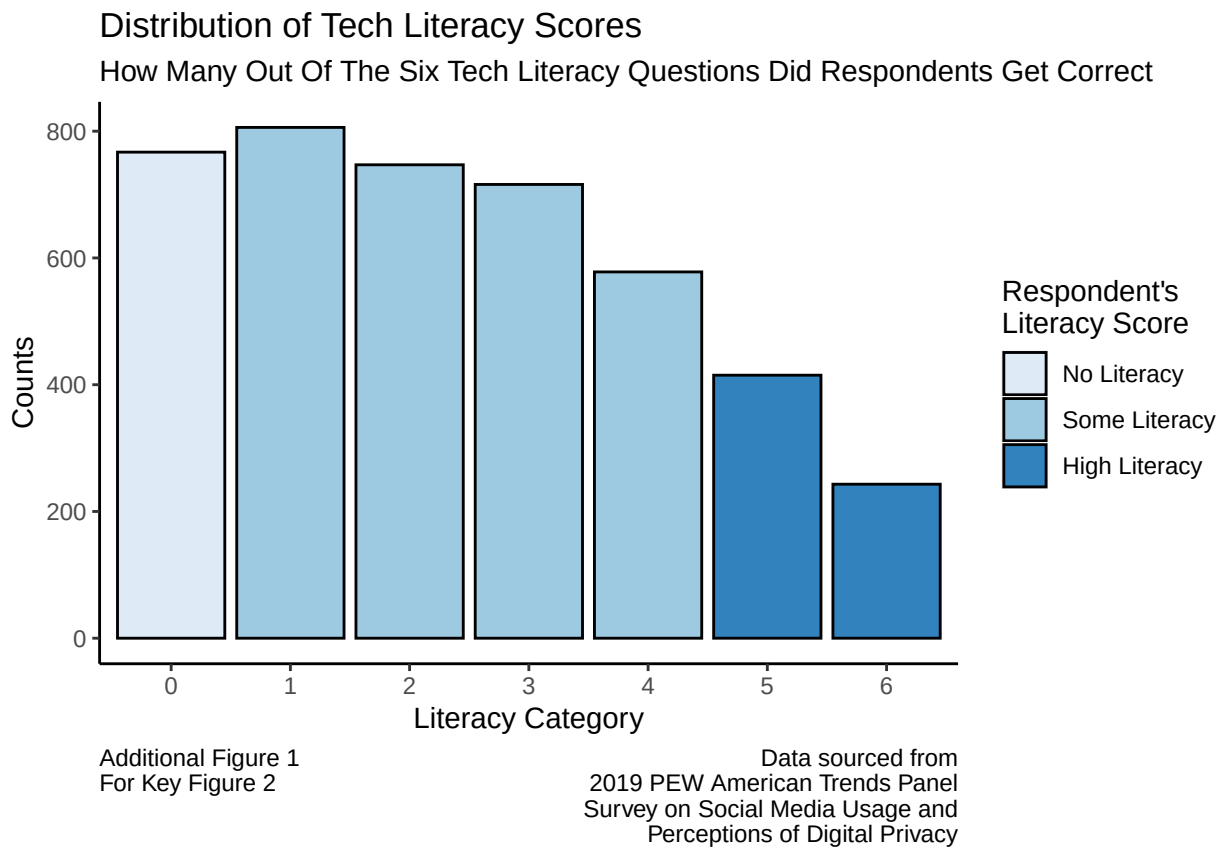
3. Underlying Distribution Of Counts For All Four RTBF Categories



Additional Figures For Key Figure 2

1. Underlying Distribution of Tech Literacy

```
## Warning: Vectorized input to `element_text()` is not officially supported.
## Results may be unexpected or may change in future versions of ggplot2.
```



Additional Figure 1
For Key Figure 2

Data sourced from
2019 PEW American Trends Panel
Survey on Social Media Usage and
Perceptions of Digital Privacy

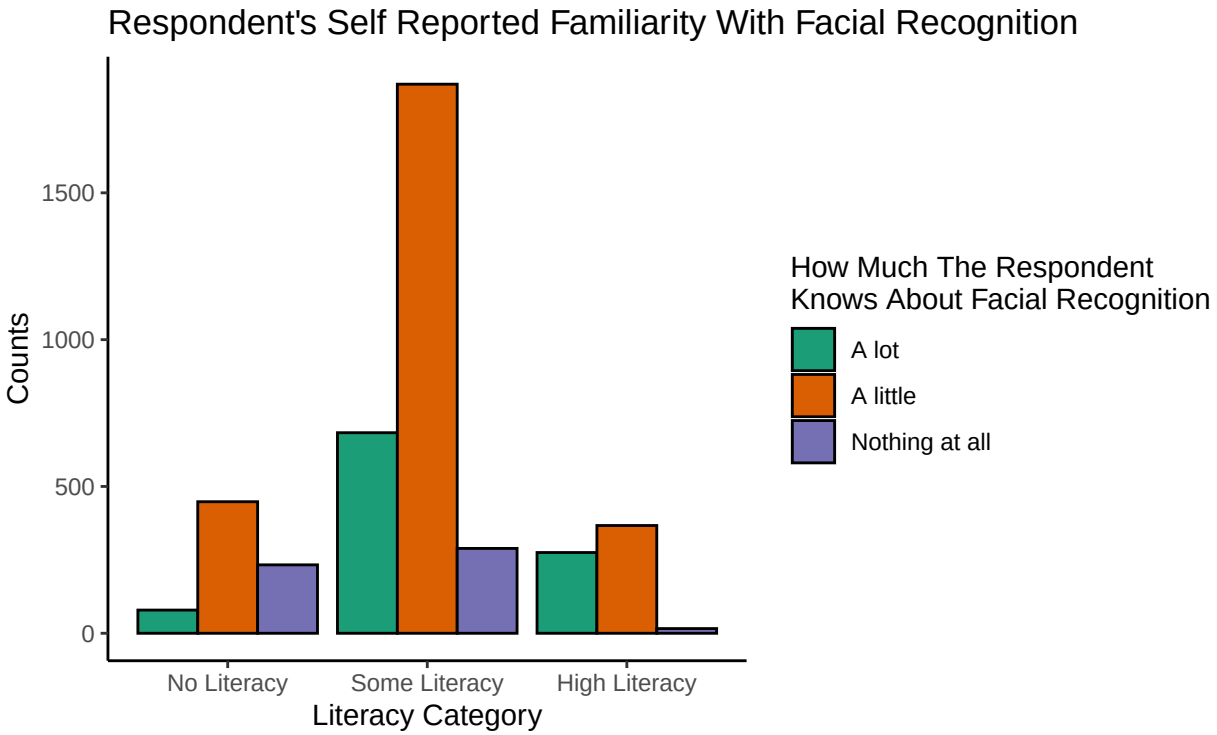
We decided to create a dummy variable that reflected how knowledgeable the respondent was about technology. The Pew survey had ten questions assessing each respondent's knowledge on topics ranging from what the 's' in 'https' means to how social media platforms generate revenue. Four of these questions – "Which of the following is the largest source of revenue for most major social media platforms?", "Where might someone encounter a phishing scam?", "Which two companies listed below are both owned by Facebook?", and a question asking respondents to identify a picture of Twitter co-founder Jack Dorsey – were excluded because they were not directly related to measuring a respondent's knowledge of how technology worked on a technical or legal level. Thus, each respondent received a literacy score between zero and six; this score was the sum of the number of questions the respondent answered correctly. The above figure, additional figure 1 for key figure 2, visualizes the underlying distribution of literacy scores.

The literacy scores are then binned into three levels – "No Literacy," "Some Literacy," and "High Literacy" – because visualizing all six levels had a poor data-to-ink ratio. The category of "No Literacy" consists solely of respondents who scored a zero out of 6, the category of Some Literacy consists of respondents whose scores ranged from a two out of six to a four out of six, and the category of High Literacy consists of respondents who scored either a five out of six or six out of six. The color in the above figure visualizes how the literacy scores are encapsulated by the binning.

After a cursory glance it is clear to see that this binning scheme puts an emphasis on those who knew nothing about the technical and legal aspects of technology. We felt that this was important to highlight because those who have no literacy are numerous and likely have a different perspective than those who have some tech literacy. We choose not to put an emphasis on those with a perfect score because the six questions we have to compute a tech literacy score measure a limited scope of knowledge and the difference between getting five or six questions correct is not as significant as the difference between answering zero or one questions correctly.

2. Self Reported Facial Recognition Familiarity

```
## Warning: Vectorized input to `element_text()` is not officially supported.
## Results may be unexpected or may change in future versions of ggplot2.
```

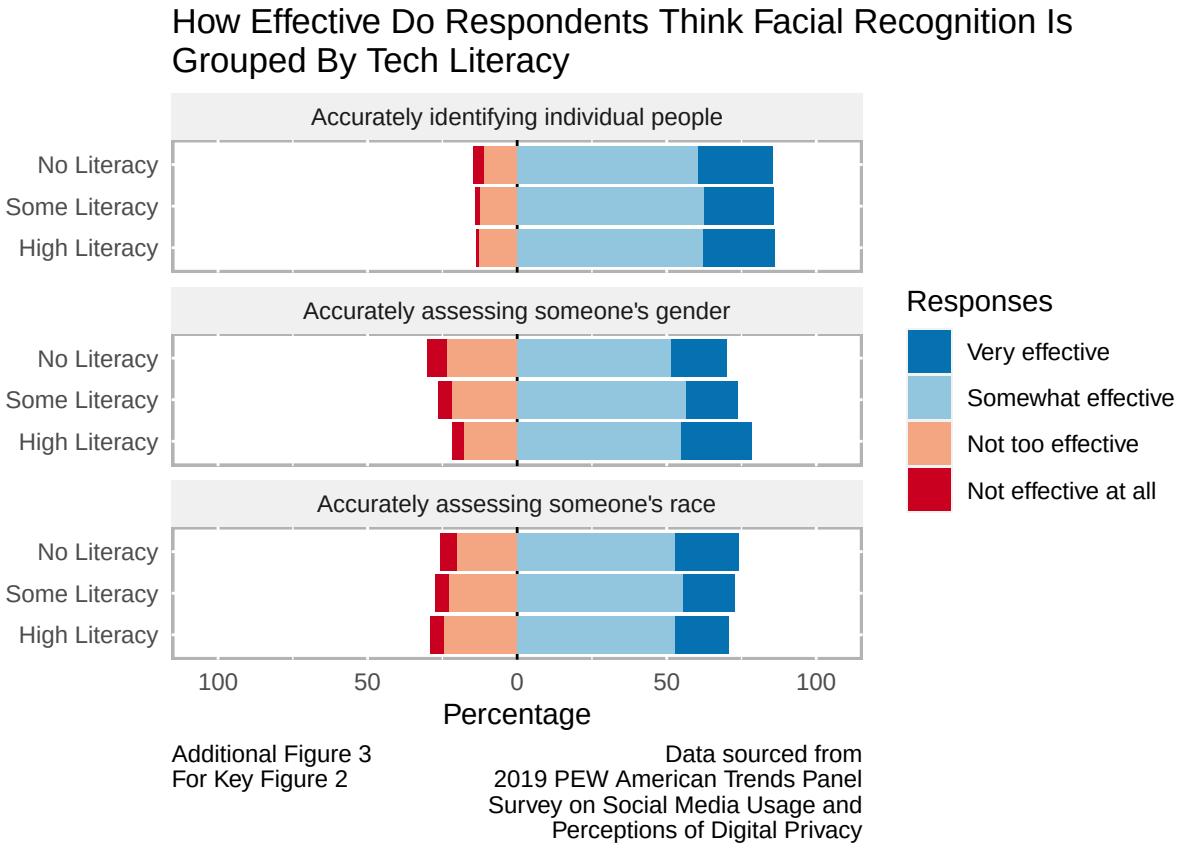


Additional Figure 2
For Key Figure 2

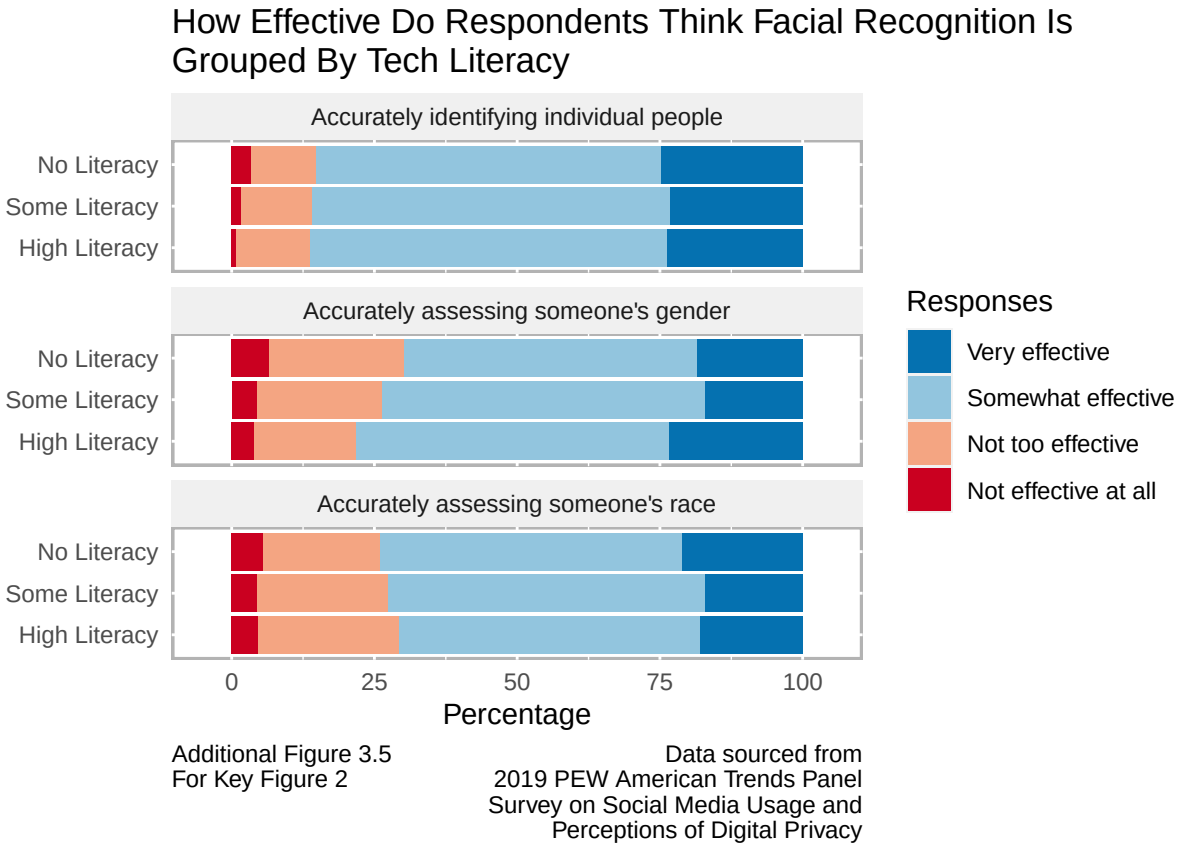
Data sourced from
2019 PEW American Trends Panel
Survey on Social Media Usage and
Perceptions of Digital Privacy

3. Respondent's Understanding of Facial Recognition

```
## Warning: Vectorized input to `element_text()` is not officially supported.
## Results may be unexpected or may change in future versions of ggplot2.
```




```
## Warning: Vectorized input to `element_text()` is not officially supported.
## Results may be unexpected or may change in future versions of ggplot2.
```

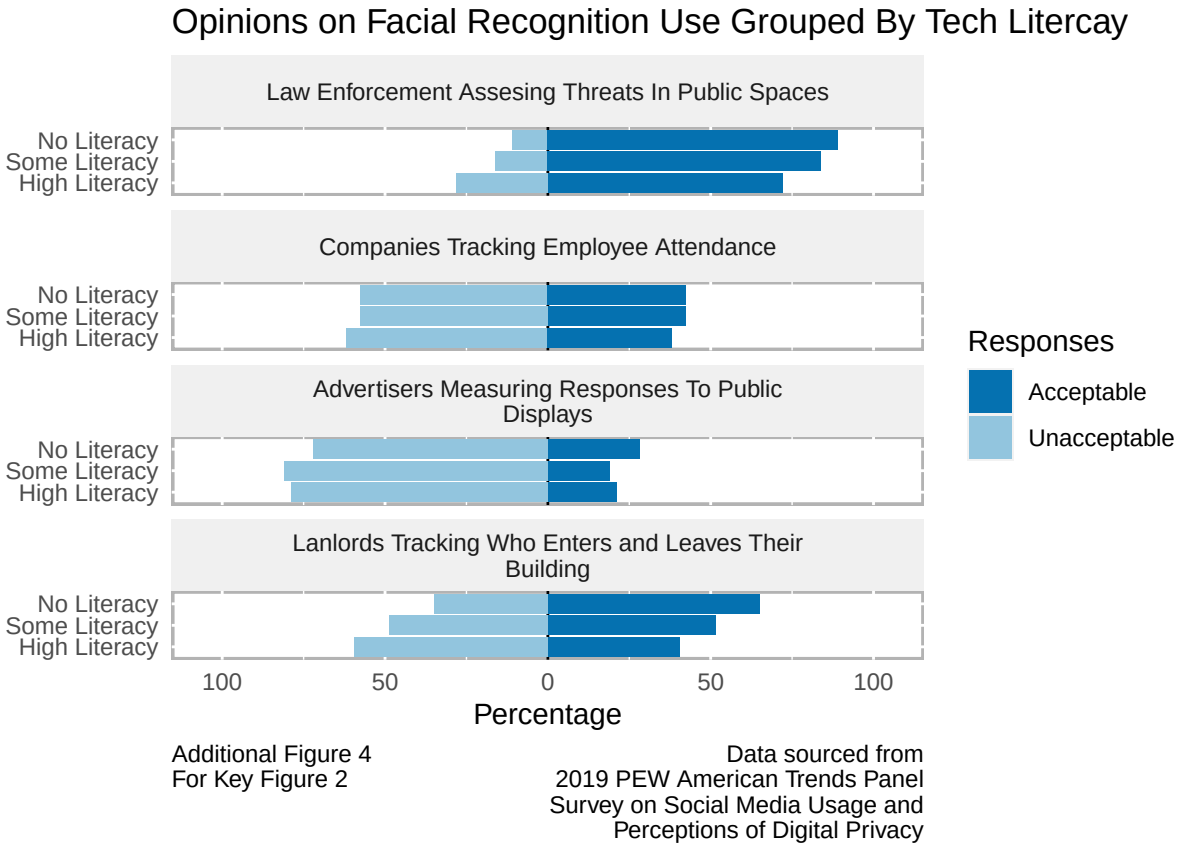


Additional Figure 3.5
For Key Figure 2

Data sourced from
2019 PEW American Trends Panel
Survey on Social Media Usage and
Perceptions of Digital Privacy

4. What Situations Respondents Think It Is Acceptable To Use Facial Recognition

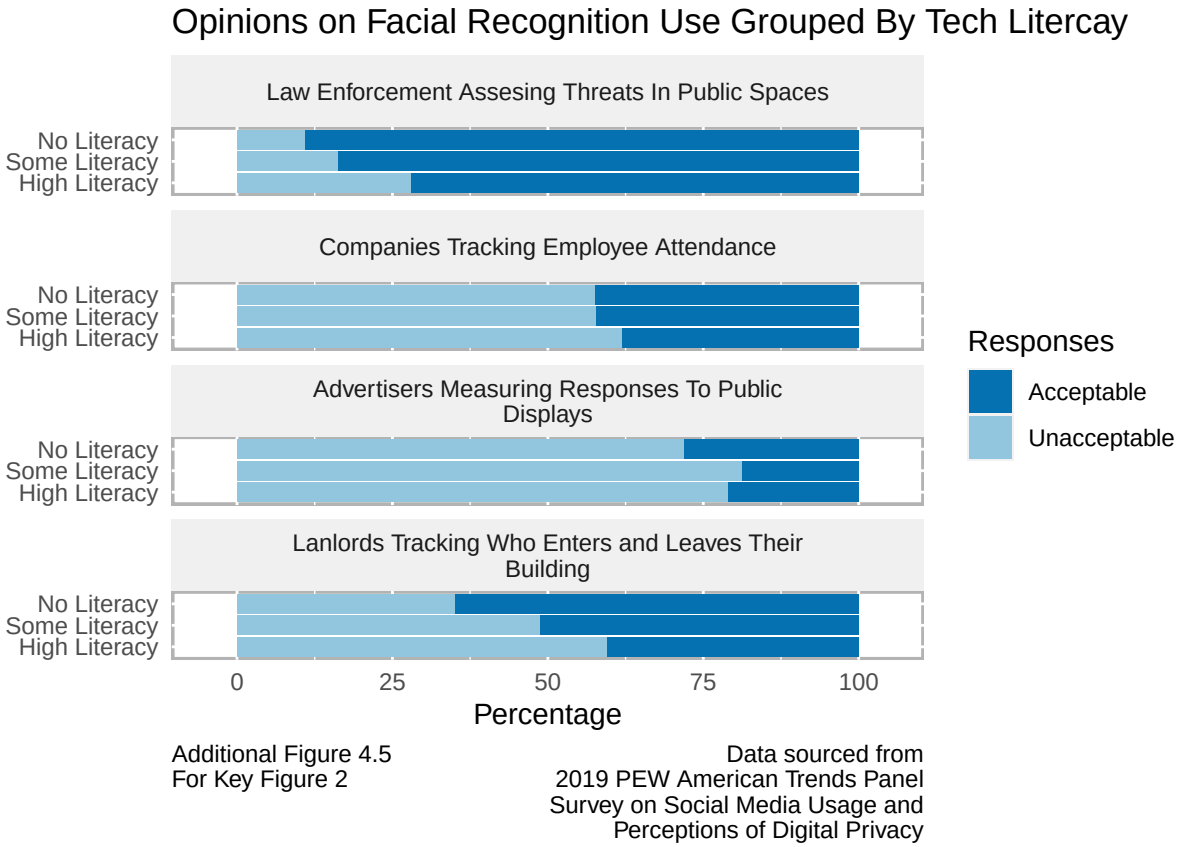
```
## Warning: Vectorized input to `element_text()` is not officially supported.
## Results may be unexpected or may change in future versions of ggplot2.
```



Additional Figure 4
For Key Figure 2

Data sourced from
2019 PEW American Trends Panel
Survey on Social Media Usage and
Perceptions of Digital Privacy

```
## Warning: Vectorized input to `element_text()` is not officially supported.
## Results may be unexpected or may change in future versions of ggplot2.
```



Additional Figure 4.5
For Key Figure 2

Data sourced from
2019 PEW American Trends Panel
Survey on Social Media Usage and
Perceptions of Digital Privacy

Additional Tables For Key Figure 1

Table 1: Summary Statistics For Key Figure 1

sumRTBF	Stance On RTBF	Freq
0	Data Should Be Private	89
1	Data Should Be Private	213
2	Data Should Be Private	442
3	Data Should Be Private	430
4	Data Should Be Private	479
0	Data Should Be Public	60
1	Data Should Be Public	97
2	Data Should Be Public	159
3	Data Should Be Public	87
4	Data Should Be Public	84

Table 2: Numeric Summary That Involves Uncertainty For Key Figure 1

publicDataNum	mean	sd
0	2.603146	1.183437
1	2.078029	1.248072

Additional Tables For Key Figure 2

Table 3: Summary Statistics For Key Figure 2

Group	Item	low	high	mean
High Literacy	Law Enforcement's Use Of Facial Recognition	46.32238	53.67762	2.461659
High Literacy	Tech Companies' Use Of Facial Recognition	71.51800	28.48200	2.018779
High Literacy	Advertisers' Use Of Facial Recognition	88.73239	11.26761	1.607199
Some Literacy	Law Enforcement's Use Of Facial Recognition	30.48829	69.51171	2.797539
Some Literacy	Tech Companies' Use Of Facial Recognition	58.59468	41.40532	2.237396
Some Literacy	Advertisers' Use Of Facial Recognition	80.26995	19.73005	1.843192
No Literacy	Law Enforcement's Use Of Facial Recognition	26.79612	73.20388	2.862136
No Literacy	Tech Companies' Use Of Facial Recognition	49.51456	50.48544	2.415534
No Literacy	Advertisers' Use Of Facial Recognition	68.73786	31.26214	2.069903

Table 4: Numeric Summary That Involves Uncertainty For Key Figure 2

Group	Item	mean	sd
High Literacy	Law Enforcement's Use Of Facial Recognition	2.461659	0.9325284
High Literacy	Tech Companies' Use Of Facial Recognition	2.018779	0.8149991
High Literacy	Advertisers' Use Of Facial Recognition	1.607199	0.6952671
Some Literacy	Law Enforcement's Use Of Facial Recognition	2.797539	0.9198941
Some Literacy	Tech Companies' Use Of Facial Recognition	2.237396	0.8672941
Some Literacy	Advertisers' Use Of Facial Recognition	1.843192	0.7908986
No Literacy	Law Enforcement's Use Of Facial Recognition	2.862136	0.9030985
No Literacy	Tech Companies' Use Of Facial Recognition	2.415534	0.8921139
No Literacy	Advertisers' Use Of Facial Recognition	2.069903	0.8637574

Discussion of Uncertainty & Inference

Key Figure 1

By grouping the data by `PUBLICDATA_W49` results and running an ANOVA test on each group's `sumRTBF` count variables, we are able to say with extremely high confidence (on a P-value that is extremely close to 0 with a value of `2e-16`) that there is a statistically significant difference between public and private data oriented respondents in the average number of categories of data they deem worthy of falling under the Right to Be Forgotten.

```
##                   Df Sum Sq Mean Sq F value Pr(>F)
## PUBLICDATA_W49    2  143.1   71.57   50.46 <2e-16 ***
## Residuals      2137 3031.3    1.42
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
## 2132 observations deleted due to missingness
```

I would like to introduce one small caveat that does not delegitimize these findings, but does complicate them slightly. Due to the nature of the dummy variable `sumRTBF`, we may know how many categories, on average, respondents identify as being worthy of protection. However, we do not know *which* categories the respondents select. There are sixteen[1] possible ways a respondent could answer the four Right to Be Forgotten questions. We know with certainty that participating respondents demonstrated trends in how

[1]calculated using combinatorics: `(4 choose 0) + (4 choose 1) + (4 choose 2) + (4 choose 3) + (4 choose 4) = 16`

many categories chosen, but we do *not* know with certainty if there are trends in *which* categories respondents chose.

Key Figure 2

Using a 1-way ANOVA test on each of the three facets in key figure 2 – Law Enforcement's Use Of Facial Recognition, Tech Companies' Use Of Facial Recognition, and Advertisers' Use Of Facial Recognition – we are able to say with extremely high confidence (on a P-value that is extremely close to 0 with a value of `1.66e-14`, `5.37e-11`, and `<2e-16` respectively) that there is a statistically significant difference in the responses of those categorized as "No Literacy," "Some Literacy, and"High Literacy" in all three facets!

ANOVA Summary For Law Enforcement's Use Of Facial Recognition

```
##               Df Sum Sq Mean Sq F value   Pr(>F)
## groupKnow      2     58  29.167      32 1.66e-14 ***
## Residuals   3719   3389   0.911
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
## 550 observations deleted due to missingness
```

ANOVA Summary For Tech Companies' Use Of Facial Recognition

```
##               Df Sum Sq Mean Sq F value   Pr(>F)
## groupKnow      2   37.5  18.763    23.8 5.37e-11 ***
## Residuals   3719 2932.1   0.788
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
## 550 observations deleted due to missingness
```

ANOVA Summary For Advertisers' Use Of Facial Recognition

```
##               Df Sum Sq Mean Sq F value Pr(>F)
## groupKnow      2   52.9  26.462   40.89 <2e-16 ***
## Residuals   3719 2406.9   0.647
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
## 550 observations deleted due to missingness
```

Discussion of Analytic Choices

Our analytical choices, while earnestly centered around most accurately representing the "truth," are imperfect. We will proceed with an explanation and critique of our analytical choices using Pierre Bourdieu's "Public Opinion Does Not Exist" and chapters 1 and 8 of *Data Visualization: A Practical Introduction* by Kieran Healy.

Per Pierre Bourdieu's article "Public Opinion Does Not Exist," our primary critique of the analytic choices that both we and the source of our data set (the Pew Research Center) made is that we are relying heavily on the survey data yielded by the 2019 Pew American Trends Panel survey as being accurately representative of "the public."

First, to echo Bourdieu's writings, we would like to problematize our use of the idea of "the public" at all; the data we have been manipulating, and the visualizations produced therein, are by no means necessarily representative of "the public." The public, as we would like to think of it, does not exist. Per the topline we received as part of this data set, the *actual* body of people surveyed is 5,869 members of the American Trends Panel: a national, probability-based online panel of non-institutionalized adults living in households in the United States, including Alaska and Hawaii. The fact that this is a pre-selected, probability-based panel highlights that the body of participants does not encompass every single person living in the United States, nor does every person living in the United States who interacts in some meaningful way with technology and digital privacy fall under those categorizations. Pew Research Center is a meticulous, thorough group known

for producing robust data as well as analyses of said data. Though, there will always be blind spots, which we must be mindful of when discussing *what* exactly our work produced.

In that regard we are guilty, also, of using this data as a means of making some grand statement about the status of society as a means of gauging "where we are" in regard to digital privacy. Bourdieu writes that "[the public opinion poll] creates the idea that a unanimous public opinion exists in order to legitimate a policy, and strengthen the relations of the force upon which it is based or make it possible" (Bourdieu 125). Not every person has or is even *able* to produce an opinion on every single question posed by the survey; this much is proved by the sheer volume of NAs in response to certain questions. We also do not know *what* those NAs even mean; Bourdieu defines the "consensus effect" to be the tendency to overlook the proportion of respondents who gave "no reply" homogenizes the populus and ignores the political reasons for certain demographics to not respond depending on the variety of question. We do not know, truly, what those NAs mean; we made the decision to largely strike them from our visualizations to help tell a better story, but that narrative in turn excludes some body whose voices we neither know nor understand, which could in turn shift our general understanding of the field of digital privacy as a whole.

The last point of contention or concern within our analysis of our data is the constantly shifting landscape of digital literacy as a whole. We are still only a few mere decades into the digital age, meaning that there is a notable generational gap in literacy, skill sets, and general understanding of the tools offered and threats posed by the digital sphere. One of our visuals does aim to gauge technical literacy, using a dummy summary count variable, though we are cautious to take it as the unchallenged truth. For those and other variables, respondents may feign understanding of topics, or answer in line to how they think they should. As such, we can at best be only cautiously optimistic about the results our analyses yield, knowing that our variables are at best approximations, and we are representing not the hypothetical, homogenous "public" but rather a pre-selected sample group.

Moving into our *visual* analyses, we turn to Healy, particularly the ideals outlined within chapters 1 and 8. Based on those readings, we took great pain thinking about presentation and accessibility in our design. The primary sins of bad design, as Healy describes them, are bad taste, bad perception, and bad data. We have done our best to address the source of data for analysis already above, and by no means cherry picked our data to further a narrative that we would prefer to tell over the one the data produced with our manipulations. For the first two, we have done our best to present the information in as clear and concise a way as we could manage. Leaning into ideas from chapter 8, we wanted to maintain not only high quality of visuals (no wasted ink, clear and regular visuals) but also accessibility. We used pre-built color palettes to display our data - sequential color palettes for unordered categorical data and diverging color palettes for ordered categorical data. In addition, it was important that we make sure our visuals were widely accessible by identifying color-blind friendly palates in colorbrewer via `display.brewer.all(colorblindFriendly = TRUE)` to select palettes that would work even for those with different abilities or perceptions. Our goal was to keep our color palette and our visual decisions at large consistent with the underlying data, visually pleasing, and accessible to all.

Discussion Of Other Ways We Could Have Made Our Key Figure

Key Figure 1

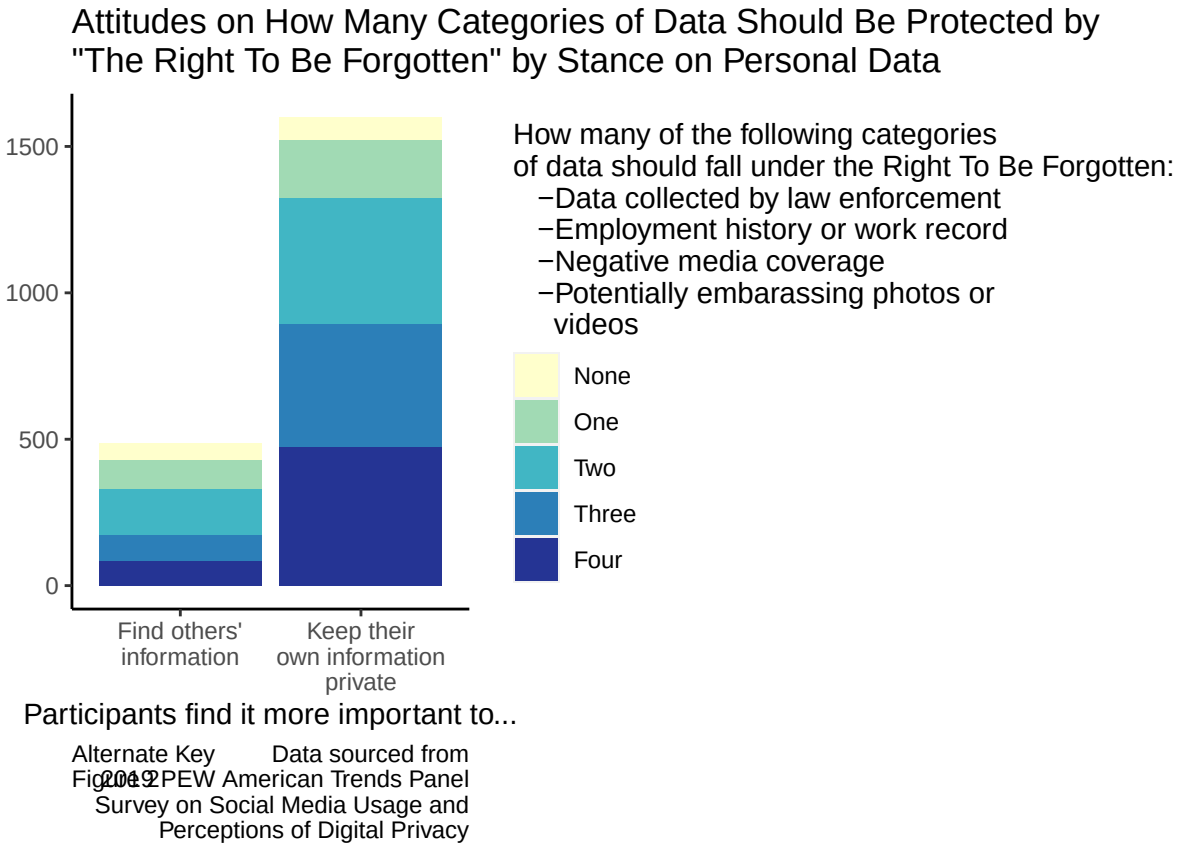
As we emphasized in the original text introducing key figure 1, there were two factors that we found it extremely important to accurately represent within our visual examining respondents' stance on digital privacy and personal data: the scale of the difference between counts for the two binary options to `PUBLICDATA_W49`, and the internal distribution for each of those two categories of respondents on the issue of the Right to Be Forgotten.

We chose fairly quickly to forgo what we would think of as the "reverse" of our final visual: a faceted bar chart broken up by the four categories of information that the survey proposed as falling under the Right to Be Forgotten, showing the breakdown of each category of data's response along the lines of those who prefer public versus private data. Though this visualization would have the advantage of showing a finer-grained understanding of the Right to Be Forgotten (showing each category directly rather than using a dummy variable of sum counts, as we ultimately did) it ultimately did not reveal anything new or interesting about

the PUBLICDATA_W49 responses. Every single response of counts only reflected the same relationship between public and private stances. This helped us narrow down our work to try and prioritize showing internal distinctions between those two categories instead.

A visualization that we considered, but rejected, is one which uses not a dodged bar chart but a stacked one, showing the two categories of public versus private data people as two bars and having those bars be partitioned accordingly to reflect the internal distribution of counts of categories that should be protected. This visualization looks as follows:

```
## Warning: Vectorized input to `element_text()` is not officially supported.
## Results may be unexpected or may change in future versions of ggplot2.
```



This visualization does both things that we would like it to do: it makes immediately apparent the difference in scale between those who prioritize public data versus private, and it has a clear color-coded breakdown of how many categories of data each class thinks should be protected. However, it is clunky and makes it harder to closely examine the distribution of sum counts than it is in our final graphic. As Healy breaks down, bad design is plagued by bad perception; stacking the boxes for each number makes it hard to directly compare the distribution of counts by not having a common base. This in turn warps our perception of the final data. So while this tells a similar story to the one up above, we ended up making additional aesthetic decisions to better convey that information in a clear and pleasing way.

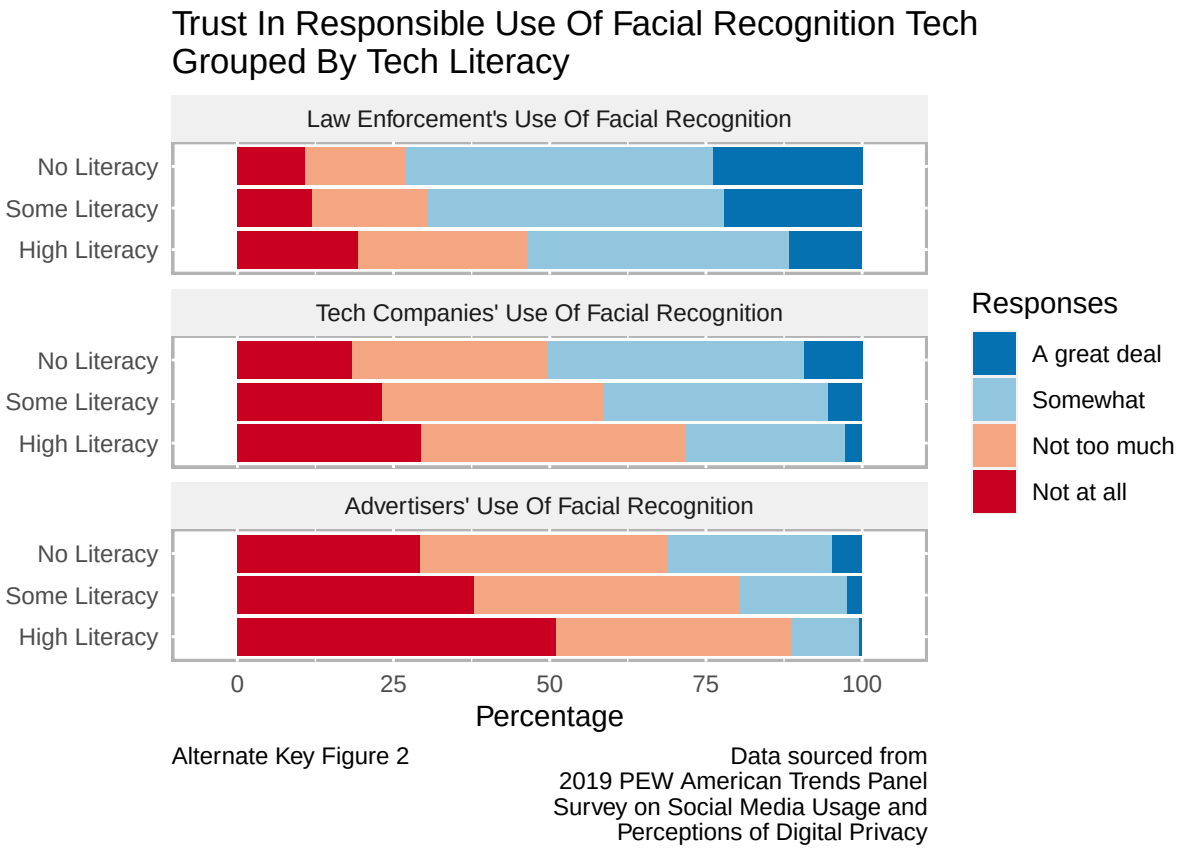
Key Figure 2

When visualizing key figure 2, I knew that I wanted to visualize some form of stacked bar chart to communicate the relative differences in comfort of various groups using facial recognition technology. Professor Ella Foster-Molina sent us an excellent article from Datawrapper making the case against diverging stacked bar charts and offering 100% stacked bar charts as the better alternative. The article argues that "the main problem with diverging bars, however, is comparability." On the whole, we agree; the most compelling point of the piece relates to how neutrals are handled in the diverging stacked bar charts. Putting neutrals in the middle

means that (1) none of the bars have a common baseline and (2) the chart is implying that part of the neutrals should be coded as positive and negative respectively. These issues are massively detrimental to making a visualization that is both easy to understand and not misleading. So, in general, the 100% stacked bar chart is the superior choice when visualizing Likert data. That all being said, none of my charts have neutrals. Thus, we think the diverging bar chart looks just fine because the overall positive-negative trend both within and between facets is more pronounced. Below is what the figure would look like with a 100% stacked bar chart.

Link to Datawrapper article: https://blog.datawrapper.de/divergingbars/

```
## Warning: Vectorized input to `element_text()` is not officially supported.
## Results may be unexpected or may change in future versions of ggplot2.
```



Distribution of Work

Jake and Adriana are best of friends and have split the work evenly. [THIS IS A PLACEHOLDER].