TRANSMITTAL LETTER

To the President, Congress, Secretary of State and the American People:

Established in 1948, the U.S. Advisory Commission on Public Diplomacy (ACPD) is authorized pursuant to Public Law 114-113 to appraise all U.S. government efforts to understand, inform and influence foreign publics. We achieve this goal in a variety of ways, including, among other efforts, offering policy recommendations, and through our Comprehensive Annual Report, which tracks how the roughly $1.8 billion in appropriated funds is spent on public diplomacy efforts throughout the world.

Part of the Commission’s mandate is to help the State Department prepare for cutting edge and transformative changes, which have the potential to upend how we think about engaging with foreign publics. This report aims to achieve precisely that. In order to think carefully about public diplomacy in this ever and rapidly changing communications space, the Commission convened a group of private sector, government, and academic experts at Stanford University’s Hoover Institution to discuss the latest research and trends in strategic communication in digital spaces. The results of that workshop, refined by a number of follow-on interviews and discussions with other organizations interested in similar questions, are included in this report.

*Can Public Diplomacy Survive the Internet?* features essays by workshop participants that focus on emergent and potentially transformative technology and communication patterns. The essays also highlight the potential challenges and opportunities these changes create for public diplomacy practitioners in particular and the U.S. government more broadly. We explore how public diplomacy practitioners can continue to productively engage with audiences around the world in the face of likely shifts in communication patterns, continue to effectively and efficiently help the United States to achieve its foreign policy priorities, and synchronize American interests with the interests of citizens and governments around the world.

Respectfully Submitted,

Sim Farar, Chair  
(California)

William J. Hybl, Vice Chair  
(Colorado)

Lyndon L. Olson, Vice Chair  
(Texas)

Penne Korth Peacock  
(Texas)

Anne Wedner  
(Illinois)

Georgette Mosbacher  
(New York)
In this essay I focus on some of the psychological aspects of how communication technology affects the way that people deceive and trust one another. The deep concerns we’ve been facing lately about a “post-truth society” are really a reflection of how we can trust one another in a world dominated by social media, a place in which people we may or may not know can communicate with us at any time and from anywhere. How can we tell if someone is lying to us in their tweet, their Facebook post, the news that they shared via a text or an online video? Worse yet, some of those people might not even be people, but bots coordinating to promote some propaganda or commercial interest.

Concerns about misinformation, fake news and whether my new friend is a bot can lead us to conclude that social media is dramatically increasing deception in the world, and that soon we’ll be unable to trust one another, or establish what information is true. But as Ambassador Bruce Wharton, Acting Under Secretary for Public Diplomacy and Public Affairs, suggests in this report, I believe that we are not in a post-truth society. Although we’re paying more attention to the topic of truth and evidence, social media and related technologies do not spell the end of honesty. Instead, that technology will transform how deception takes place, how we detect lies and how we come to trust one another.

These changes to truth-telling and trust will not be random or unpredictable, but will be driven by principles and factors that the social sciences have been identifying over the past century. We need not throw out the book of psychology, for example, to understand how public diplomacy needs to adapt to the changes wrought by social media. Below I review these principles and provide an overview of the latest research on deception detection and trust, concluding with insights on what those engaged in public diplomacy need to address most to succeed in an evolving communication and information environment.
An overall meta-analysis of hundreds of deception experiments reveals that humans perform at chance levels (54 percent) when detecting deception. We really aren’t very good at telling if someone is lying based on verbal or nonverbal cues, in part because there are no reliable cues. This difficulty in detecting deception transfers over to social media deception. In studies examining phishing attacks, where deceptive emails are used to access sensitive information (as was the case in the hacking of the Clinton campaign accounts), even sophisticated users can be deceived, online or off.

In fact, there is only one reliable finding in every deception detection study: people tend to trust what others say, an effect called the **truth bias**. Our default state is to trust what other people say. This bias is deception by just relying on cues in the message, we now have information tools available that can help investigate potential deceptions that were hard to imagine just a few years ago (for more on the value of fact-checking efforts, see Ethan Porter’s essay in this report).

The last finding from the deception literature that is important to share is that people lie for a reason, and these reasons are widely varied. While this may seem obvious, it is important to note this when considering how deception operates in the current environment. Fake news articles in the last election cycle were produced sometimes to influence voters, but more often the motives were simply profit. Without considering the reasons for deception, it is impossible to counter them.

"Every generation tends to think that the current generation is less honest than the previous generation. This is an old human concern."

actually quite rational—most of the messages that a person encounters in a day are honest, so being biased toward the truth is almost always the correct response. This tendency to trust messages is, of course, one of the reasons that lies can succeed, but it’s important to note how fundamental the truth bias is. Language philosophers even argue that for language to work we must assume a cooperative partner, suggesting that the truth bias is fundamental to communication.

There are two other important findings from the deception literature that are relevant to public diplomacy. While we have a difficult time detecting deception from cues, like eye gaze or vocal pitch, people can detect lies when they have the time, resources and motivation. Lies are often discovered through contradicting information from a third source, or evidence that challenges a deceptive account. Much like the way police officers investigate witness statements and suspect alibis, people often determine that they have been deceived by seeking out and learning from other information. Our recent work suggests that most lies that people detect rely on information from others, or come from using search engines like Google or examining activities posted on social network sites like Facebook. Thus, while we may be bad at detecting...
across sources. Thus, while our default is to trust incoming information, people also evaluate their information environment to ensure that their understanding of their world is valid.

As our information ecology evolves to be more mediatized and digital, the operation of epistemic vigilance needs to evolve as well. Consider the sharing of a fake news story by Shawn on Facebook that is read by Markos. There are several signals Markos’ epistemic vigilance might rely on: the degree to which Markos knows and trusts Shawn, how often the article has been “liked” by others, and the number of times the article has been shared. If these signals are all high, then there is little to trigger additional vigilance or signal for Markos to move away from his default state of trust.

Since the alarms over fake news emerged, social network sites and journalists have begun to develop additional signals that can help people assess the validity of information. For example, Facebook now allows users to flag stories that may be fake. These stories are then examined by fact checkers, and if the story is fake an alert is shown whenever the story is shared on the platform. This kind of signal functions to trigger epistemic vigilance and help individuals make decisions about whether to trust the information or not. While this is a promising development, it is still too early to measure the effectiveness of these measures. This change nonetheless points to at least one direction for improving our ability to assess information in social media.

Much more is required to establish trustworthy communication in our evolving information environment. While substantial work is required to continuing improving the trustworthiness of our cyber systems, we also need to better understand the social aspects of these new technologies. In our own work, we have begun to look at how people reason about social technologies, like Facebook or Twitter newsfeeds. We find that people have folk theories about these technologies, which represent the person’s general understanding of how a system works. These theories weigh questions, such as: How do algorithms decide to share info? How are sources perceived? To what degree do these systems validate information?

For example, we find that some people think of Facebook’s newsfeed as a personal shopper, helping the person find things of interest to them. Others, however, think of the newsfeed as a spy or as paparazzi, concerned that the system is designed to exploit them for the gain of others. Without knowing more about people’s folk theories of these complex systems, it is difficult to predict how audiences will react to messages that are shared through them, such as whether they trust them or not.

**SOME REASONS FOR HOPE: LESSONS FROM THE SHARING ECONOMY**

There is substantial reason to be optimistic in the long term about truth and trust with technology. Although trust in institutions, such as media, government and religion, has been in decline for over a decade, there has been substantial trust observed in how people are believing each other via technology. For example, when purchasing new products and services, most people will rely on online reviews to make decisions about what hotel to reserve or which car to buy. More people trust peers when making these decisions than any other form of media. In another domain, we see huge trust in social support groups that operate on the internet, with strangers providing support and advice to other strangers, trusting one another to help each other face cancer, overcome the loss of loved ones, or how to recover from bankruptcy.

This inversion of trust, decreasing trust in institutions but rise in interpersonal trust, can also be observed in the sharing economy, from home-sharing to car-sharing. Consider the level of trust required to allow strangers to stay in your home. Or the amount of trust required to hop into a stranger’s car late at night in a strange neighborhood. How does trust operate in this multi-billion-dollar economy, and what insights can it provide for public diplomacy in this evolving communication environment?

First, the trust placed in these services is warranted. Very few rides on Lyft or Uber result in any negative incident. The same is true for house-sharing services like Airbnb. One reason for this is that the users’ goals are aligned. One user would like to sell their service while the other user wants to buy this service. When goals are aligned, trust can facilitate many social transactions. Public diplomats know this well—messages must be aligned with the goals of the audience or the partner. Forgetting this can undermine any diplomatic enterprise.

Second, while we usually think about the person taking the risk when we think about trust situations, it is important to consider the psychological dynamics on the other side of the risk, the person being trusted.
When people are trusted with something valuable, such as being allowed into a stranger’s home, they often experience feelings of responsibility and are even nervous about harming the other person. Indeed, many Airbnb hosts report that their homes are in great shape after renting them out. Trust often leads to trustworthy behavior.

Third, users of these services believe that there is infrastructure in place to protect them from violations of trust. Users expect that brands like Airbnb will reimburse them for any damages. Further, there trust is built on layers of older, legacy infrastructure, like law enforcement and financial regulation. In addition to the brand of a service, such as Airbnb, users expect to be supported by the enforcement of legal institutions put in place long before social media came on the scene, from the police department to the Consumer Financial Protection Bureau. These layers of infrastructure that build trust should also be considered in public diplomacy campaigns. Programming that aims to establish relationships, and build on those relationships over time, is likely to result in robust networks of shared interests and understanding.

Finally, technology plays an important role. Users of Uber report feeling safe in part because the app constantly records where they are. They believe that should something go wrong, there will be a record, and that this record keeps people honest. Indeed, one of the most important transformations of the communication environment is the record of behaviors, taking millions of rides with strangers and allowing millions of strangers to stay at their homes.

**LESSONS FOR PUBLIC DIPLOMACY: TRAINING AND IMPLEMENTATION**

As people engaged in public diplomacy adapt to the evolving communication environment to engage with foreign audiences, what are some of the keys for success? The first is recognizing that the goals and values of the United States and its allies and adversaries are paramount. It is important to keep a focus on goals, objectives and our own values. Deception is often detrimental in the long term, and the costs to reputations can be severe. In one study asking people to rank traits, the one ranked lowest from a total of over 500 was “liar.”

It is also important for those serving in a public diplomacy role to receive new forms of training and education. This training should involve an emphasis on media literacy, including both the social science of technology and also enhancing technical skills. One model may be the computational journalism program at Stanford University, which seeks to transform journalism by providing journalists with computational capacities that will change how they can investigate issues of public interest. I can imagine a new program for “computational diplomacy” that has similar goals, to develop new skills for diplomacy that incorporate computational abilities and social science training for understanding the social and technical aspects of new communication environments.

Finally, the United States needs to continue to develop its technical capabilities to be able to detect and counter misinformation and other attacks by hostile others. Importantly, this should be coupled with a similar investment in training in the social sciences, from the psychology of technology discussed here to social network analysis. All of these technological capacities and social analysis skills will be required to best engage our foreign audiences.
ENDNOTES

1. In media studies, mediatization is a theory suggesting that the media shapes and frames the processes and discourse of political communication as well as the society in which that communication takes place.