CDA INSIGHTS 2020

EXECUTIVE SUMMARY

USER PERCEPTIONS OF TRUST AND PRIVACY ON THE INTERNET

BY KRISTEN ROGGEMANN, GALIA NURKO, AND ALEXANDRA TYERS-CHOWDHURY

OCTOBER 2020

DAI
Shaping a more livable world.

CENTER FOR
DIGITAL ACCELERATION

DAI's Center for Digital Acceleration helps our clients integrate digital tools and approaches across their portfolio, especially in emerging markets. We do this by engaging end users, building digital products, and understanding the broader ecosystems that drive the success of technology-based initiatives. Our clients include bilateral and multilateral donors, private sector companies, foundations, and others seeking to drive positive social change across a cross-section of sectors including health, governance, agriculture, education, and economic growth.

Design: Jennifer Geib, www.jennifergeib.com

The internet unlocks economic opportunity and access to critical services for populations around the world—including for unserved and underserved communities. However, a digital divide continues to separate those who have access to digital tools and services from those who do not. As efforts to bridge this divide succeed and more people come online, the number, variety, and severity of digital risks is also rising, sowing distrust in the digitally enabled tools and services on which so many of us rely.

Trust underpins digital adoption. Therefore, a decline in trust poses a stark challenge to national governments, international donors, and private companies seeking to promote digital inclusion. If digital distrust erodes confidence to the point where the unconnected or newly connected are deterred from using the internet, the digital divide will grow, and more people will be left behind at the very time our economies are becoming more digitized. Such deterrence effects have a particularly adverse impact on more vulnerable populations in emerging markets, such as women and girls. To fully realize the potential benefits of internet access, we must match our investments in digital infrastructure, digital tools, and digital services with a commensurate investment in digital trust.

To date, most efforts to sustain trust focus on supply-side interventions to mitigate digital risk. A mobile technology company might repair a coding vulnerability that accidentally exposes people's data; an enterprise may require employees to use two-factor authentication to sign in; a social media giant might develop an algorithm to identify disinformation; or a government may configure its email domains with a validation solution such as DMARC to prevent fraud. These UX/UI and back-end interventions to strengthen online security and privacy are important but represent only half the equation. What's missing is the demand side: how *users* understand the challenge before us.

Today, we lack good data on how users themselves perceive privacy and security online and how that shapes their trust of the internet. By interviewing urban youth in Accra, Ghana and Chennai and Delhi, India about this very issue, DAI hopes to advance the conversation beyond supply-side solutions to encompass demand-side insights that deepen our understanding of whether and why users trust, or don't trust, the digital information and platforms they encounter, and what tactics they use to protect themselves online.

If digital distrust erodes confidence to the point where the unconnected or newly connected are deterred from using the internet, the digital divide will grow, and more people will be left behind at the very time our economies are becoming more digitized. Such deterrence effects have a particularly adverse impact on more vulnerable populations in emerging markets, such as women and girls. To fully realize the potential benefits of internet access, we must match our investments in digital infrastructure, digital tools, and digital services with a commensurate investment in digital trust.

Four thematic areas of exploration

While not nationally representative, the qualitative interviews nevertheless yield valuable insights and highlight commonalities worthy of further exploration across four thematic areas: 1) perceptions of privacy and offline influences; 2) trust of online information; 3) tactics to protect privacy and security online; and 4) gender dynamics. We learned that for urban youth respondents in Accra, Chennai, and Delhi:

1. Perceptions of privacy online are significantly conditioned by factors—perceived or real—in the offline environment, particularly factors such as the attitudes of authority figures (including religious leaders), family members, and significant others. Socio-economic, political, and cultural influences will often lead people to create distinct online "identities" to protect their offline reputation.

2. The existence of mis/disinformation is widely known, yet people's perceptions of what is often dubbed "fake news" – and of how much risk it presents to them personally – vary by geography and depend on how well they understand how digital platforms operate.

3. Tactics to protect privacy and security online differ depending on whether users own their smartphone or share it, on whether they are male or female, and on their level of digital literacy. Users might invent codenames for contacts of the opposite sex, for example, or change mobile application settings, or limit the types of information they share on digital platforms.

4. Offline gender gaps and dynamics influence perceptions of security and privacy online, affecting what digital services women can use and how they use them compared to men. All participants voiced concerns about the offline consequences of online behavior, but those perceptions most acutely limit what women do online, which risks exacerbating the online gender gap and leaving female internet users even further behind.

Recommendations

Based on these findings and the existing literature, we offer the following recommendations:

- The digital development community should adopt a 10th Principal for Digital Development focusing on advancing digital and media literacy for the user.
- The digital development community should drive coordinated, cross-sector action to develop and adopt universal (but "localizable") digital and media literacy curricula in an open-source, dynamic fashion.
- Technology companies, especially global platform providers such as Facebook and Google, should guard against assuming that Western norms apply universally by increasing investment in localized design research and robust user testing when developing privacy solutions for global audiences and marginalized groups.
- The international development community should fund additional research to better understand privacy and security from a user's perspective, taking particular account of women's views, and exploring diverse geographic, socioeconomic, and demographic settings.
- Regulatory bodies should engage a diverse group of stakeholders from across the public and private sectors, academia, and civil society to develop fair, innovation-friendly, yet protection-focused privacy and security policies that strengthens an open, interoperable, peaceful, inclusive, and secure internet.

In working to increase digital inclusion, focusing on demand-side issues shines new light on how best to maintain trust. We hope our approach informs and provokes further conversations between technologists, international development practitioners, and policy makers, and encourages them to renew their attention to new, veteran, and even unconnected users.

Want to learn more? Read the full report here »

Let's continue the conversation on our Digital@DAI blog and social media channels.

BLOG | TWITTER | PUBLICATIONS | FACEBOOK | LINKEDIN | INSTAGRAM

SHAPING A MORE LIVABLE WORLD.

www.dai.com

@daiglobal