TRUST:
THE FOUNDATION FOR SERVING CITIZENS IN A DIGITAL WORLD
Trust—it’s a concept that is inherently nuanced. What, exactly, does it mean to trust a person or an institution? Are there degrees of trust? How is trust earned? How is it preserved over time?

Though challenging in any setting, trust is especially complex in a digital context. We often have less confidence that our online counterparts are acting honorably due to the relative anonymity of the Internet. And our faith in the systems that house our most intimate information is shaken daily by reports of continuous breaches, cyber-attacks and the schemes of bad actors.

Those risks exist alongside powerful opportunities to use the Internet and social media as vehicles for fostering stronger, deeper, and better relationships among individuals and with the organizations that serve them.

Government, of course, is not immune from the nuances or challenges of trust. In an October 2017 survey by Government Business Council and Accenture, 77 percent of federal respondents reported that citizen trust in government is weak or weaker than ever.¹ A recent Pew Research Center study found that roughly half of Americans do not trust the federal government to protect their data.² And yet, there is hope for improvement. In another Pew study, nearly half of respondents (48 percent) indicated a belief that over the next 10 years, people’s trust in online interactions will be strengthened.³

Here’s how government can support that shift—and why it matters so much.
Citizen trust has several critical dimensions. First, citizens need to have a fundamental trust in government and each agency’s ability to deliver services and solve problems as promised. Second, citizens need trust specifically in digital government and an agency’s ability to adequately safeguard personal, and often sensitive, information. Finally, citizens need a way to verify that communications—email and text messages, websites, and phone calls or letters directing them to online sites—are indeed from real and trustworthy government sources.

Those challenges are compounded as agencies move to increase the level of personalization in digital interactions. From integrated records that provide a broader view of a client’s situation to dynamically tailored website content, increased personalization is a worthy aim. After all, it helps citizens engage and conduct business with government more quickly, conveniently, accurately, and efficiently. What’s more, personalization is increasingly critical to meeting expectations shaped by experiences with leading commercial services tailored to individual customers’ needs and preferences. Greater personalization of government services will require greater trust from citizens and the assurance that both their privacy and security are protected.

In working to fuel digital transformation, every agency faces this fundamental question: How can we balance the need for privacy with the goal of delivering a simple, seamless, and convenient customer experience?

Achieving and maintaining that balance requires active collaboration between those responsible for privacy and those charged with delivering citizen services. As they pursue mutual goals, they must recognize differing priorities (“We need personalization” and “We must protect information”). Even in the context of privacy, there are differences of opinion between those responsible for deciding how data can be used and those entrusted with protecting it from unauthorized use. Viewing digital transformation through the lens of citizen trust raises opportunities to build confidence both among the public and within an agency’s workforce to balance these priorities.
WHERE TO START

1 UNDERSTAND—AND MEET—YOUR CITIZENS WHERE THEY ARE

Gain insight on the context of the engagements citizens have with your agency. Understanding that will help you design the expectations of citizens’ experiences with your agency. Consider developing personas, customer experience (CX) journey maps and comprehensive service blueprints to understand and address citizen needs at scale. Fortunately, mapping these insights with virtual settings can provide an opportunity for trust to be negotiated and nurtured — especially with entities that people do not physically see. At the same time, recognize that while building trusted interactions with citizens digitally will be an ongoing need, building trust in interactions offline will continue to be important. That is especially true for tougher-to-reach audiences.

2 GIVE THE PEOPLE THE POWER

Empower citizens by simplifying and explaining in plain language the often-complex process they are engaging in. Give them the ability to opt in and then help them understand what opting in means for them, how the information will be used, what to expect next and what their participation will enable.

3 COMMUNICATE THE BENEFITS

Educate citizens about how their information will be used, why, and how it can benefit them. Citizens may be more willing to engage digitally when they gain something in return—which is faster processing or more personalized content or attention. For example, in the commercial world two-thirds of consumers are willing to share personally identifiable information (PII) in exchange for some perceived value. One-quarter are willing to share PII for a higher level of service or the ability to choose which data is shared with third parties. Remember: Communication is two-way, and citizens have plenty to say. Acknowledge their feedback and address their concerns—whether they are personal questions or issues in times of crisis. Every time you handle those situations well you build or reaffirm trust.
4 BE TRANSPARENT

Demystify the digital experience. Share the movement of processes and be clear about data usage intentions. Empower citizens to feel ownership and have access to their records at their convenience. Just as important, take ownership when things go wrong. A swift, decisive response lets citizens know safeguarding measures are in place, advances are to come, and citizens’ concerns are being heard and addressed. In fact, Accenture research showed that in four of 10 cases, consumer trust in a company increases when breaches are handled swiftly and correctly. This kind of transparency is vital to helping overcome obstacles to citizen trust.

5 BUILD IN PRIVACY AND SECURITY

Technology is continually advancing, and there are new and increasingly effective ways to support trust. For example, agencies are adopting two-factor identity authentication to provide assured identity in a scalable, non-invasive way. Blockchain technology has shown promise for being especially useful in protecting PII. Use it to track digital transactions and store digital records with some key properties—including immutability, decentralizations, and tamper-evidence. Meanwhile, ensure privacy and security are also central to the organization’s culture. Every person in the agency workforce should be making decisions and taking action through that lens.

Whether in personal relationships or public service, trust is built and maintained over time. It is essential to mutually beneficial outcomes. Keep citizen trust top of mind to realize the greatest value from your digital transformation.
CONTACT THE AUTHORS

Kathy Conrad
Director, Digital Government
Accenture Federal Services
kathy.conrad@accenturefederal.com
@kpconrad
/kathypconrad

Jen Combs
Managing Director, Security
Accenture Federal Services
jennifer.l.combs@accenturefederal.com
@jln_combs
/jennifer-combs-7673047

NOTES

1 Citizen Trust Survey, Government Business Council and Accenture, conducted October 2017

2 Americans and Cybersecurity,” Pew Research Center, retrieved 31 October 2017 from Americans and Cybersecurity

3 “The Fate of Online Trust in the Next Decade,” Pew Research Center, retrieved 31 October 2017 from The Fate of Online Trust in the Next Decade

4 A New Slice of PII with a Side of Digital Trust,” Accenture.com, retrieved 31 October 2017

5 “A New Slice of PII with a Side of Digital Trust,” Accenture.com, retrieved 31 October 2017

ABOUT ACCENTURE FEDERAL SERVICES

Accenture Federal Services, a wholly owned subsidiary of Accenture LLP, is a U.S. company with offices in Arlington, Virginia. Accenture’s federal business has served every cabinet-level department and 30 of the largest federal organizations. Accenture Federal Services transforms bold ideas into breakthrough outcomes for clients at defense, intelligence, public safety, civilian and military health organizations.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 425,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

Copyright © 2017 Accenture
All rights reserved.
Accenture, its logo, and
High Performance Delivered are trademarks of Accenture.