CHAPTER 5

When, How, and Why Do We Trust Technology Too Much?

Patricia L. Hardré
University of Oklahoma, Norman, Oklahoma, USA

People working in technocentric and technology-heavy fields generally know enough about technology failures to embrace reasoned skepticism and exercise abundant caution. However, many people rush to use and implement new digital technologies without really understanding them. Technology is often adopted with an absolute faith approaching religious zealotry. Organizations, institutions, businesses, and government agencies use digital systems to save time and money, reduce paper management, conserve environmental resources, and extend their reach to distributed customers and users. Too often these digital systems, complex in ways that even the owners and administrators fail to understand, receive an absolute level of trust, well beyond their actual power, security, and stability. Technology overtrust is an error of staggering proportion, the direct and residual effects of which have become apparent locally, nationally, and internationally.

When technology experts meet, stories frequently center around gaps between expectations and reality for technology users. One such story is my own recent experience, of 16 members of a national committee choosing to use a new technology tool for a virtual meeting, *intended to improve* communication and efficiency.[1] However, getting the group up and running occupied half of the time allocated for the meeting—an actual result in *reduced* communication and efficiency. Another horror story shared by

[1] Individual examples cited in this manuscript are from published news stories or online postings, personal experiences, or stories shared in public contexts. Some of these stories were shared in sessions at 12 different education and technology professional conferences, with no expectation of confidentiality. The author collected them systematically as data on this topic. Even so, those that have not been published have been anonymized to protect participants' identities, and they are presented as exemplars of events that may occur frequently.

Emotions, Technology, and Behaviors
http://dx.doi.org/10.1016/B978-0-12-801873-6.00005-4

a colleague was about the college that converted all its old paper student records to digital archives, and then had a power failure that fried the archives—without an off-site backup. Tech terror stories abound when natural disasters occur, but also just in the rhythm of risks people take in daily life and work. Yet even when technology works as it was intended to, a broader look at human interactions with these systems, our responses to them, and the effects they have on us reveal reason to be concerned. It is possible that we may simply trust our technologies too much for the good of all concerned.

From the individual who trusts her cell phone as the only storage place for contact data, to the U.S. Office of the President trusting the readiness of its national healthcare enrollment system; from the university students that trust the digital citation database to be current and accurate, to Target stores and customers trusting the security of its credit card data—so many examples illustrate the tendency of people to overtrust digital tools and systems. And when these tools and systems fail, the impact is wide and deep, as the backlash from overtrust to lack of trust turns on the organizations and institutions that owned and sponsored those failed systems.

This chapter examines issues surrounding the trust, and often overtrust, that individuals and groups in society bring to their interactions with digital tools and systems. This chapter will decompose and examine questions of trust in technologies, whether we (as individuals and as a society) buy into digital technologies too readily and trust them too implicitly, along with what social and emotional factors appear to influence these tendencies. In addition, this chapter considers what implications these patterns of trust have for human behavior and consequently for organizations. Grounded in trust theory and research, this chapter will examine six key dimensions of overtrusting technology.

1. Two outcome dimensions: (1) the technology's functionality (trusting that it is working or has worked) and (2) trusting the information that it provides (without alternative sources of verification).
2. Two perspective dimensions: (1) the end-user overtrusting (resulting in lack of backup or alternate access planning) and (2) IT support staff overtrusting (resulting in overlooking possible system errors and tendency to blame the end-user first when complaints are reported).
3. Two critical process dimensions: (1) overtrusting system security (resulting in reduced vigilance leading to crisis and damage control) and (2) overtrusting the utility and intuitiveness of user-side features in new digital systems (resulting in oversights with important consequences).

Although it will not be possible to fully develop and elaborate all these issues here, it will be possible to explain and illustrate the phenomenon of over-trusting digital technology tools and systems, its processes, and its individual and social consequences.

AUTHORIAL PERSPECTIVE

Part of scholarly responsibility and transparency in an interpretive work of this kind includes explicitly framing the authorial perspective. Something of an oddity in the field of Instructional Psychology and Technology, I am neither a technophile nor a technophobe. I do not grab onto the latest digital gadget because it exists or because I can, but I do not shrink from or resist new digital or nondigital change just because it is different. I weigh the advantages and disadvantages of technologies on a case-by-case basis and use technology when it actually addresses a challenge or solves a problem, where it facilitates efficiency and effectiveness. I operate on the premises that no digital system is functionally perfect or absolutely secure, and that all technology tools and systems come with learning curves. In a world rushing to embrace the newest digi-gadgets at every turn, instilling a little reasoned pause seems like a healthy and balanced approach. Given recent indicators, from crime and crisis reported in the daily news, to anecdotes reported online and by the water cooler, it is clear that people trust digital tools to an amazing extent. However, we may want to consider the potential that, and effects if, we place *too much* absolute trust in our technology systems.

THE NATURE AND COMPONENTS OF TRUST

Trust is a complex, multidimensional psychological construct that drives human behaviors (Kramer & Carnavale, 2001). Elements of the trust dynamic draw from the disciplines of psychology and sociology, as applied to educational, work, and family relationships (Simpson, 2007). Fields that draw on the concept of trust offer differently nuanced definitions, but these converge on an essential meaning, that trust is confidence that one will achieve desired outcomes, rather than experience feared costs or reprisals, when dependent on an agency outside of self. As such, it constitutes an interaction of people's values and hopes with their insecurities and fears (Simpson, 2007).

Trust is not itself an emotion, but it is closely related to emotions, arises from and evokes them, and is embedded in perceptions and responses, which

function dynamically and reciprocally as antecedents to and products of trust (Simpson, 2007). Trust drives romantic attachments, workplace partnerships, business arrangements, education, and recreational connections (Holmes & Rempel, 1989; Mikulincer, 1998). Trust is a critical factor in all types of relationships (Montague & Asan, 2012) and in actions that result from them. Outcomes of trust include adoption, investment, cooperation, giving over control, risk-taking, innovation, and improved performance (Krieger, 1997).

The study of trust originated with interpersonal human relationships, grounded in theories of psychological development (Erikson, 1963) and focused on the trust of individuals and groups toward one another in daily life. Today, digital technologies, both tools and systems, function as replacements for trusted human roles (Turkle, 2011). Some of these roles include education and information access, safety and security, financial transaction and money management, transportation, communication, and health care (Xu, Kim, Deitermann, & Montague, 2014). Relative to its current importance in human life and action, research on trust is limited (Simpson, 2007), and research on technology trust has not addressed its full complexity or impact (Montague & Chiou, 2014).

Trust involves vulnerability to disappointment or harm and expectations of how the trusted-other will function in terms of the trustee's needs, interests, and benefits (Kramer & Carnavale, 2001). Individual differences in familiarity, past experiences, self-esteem, personal confidence, and risk tolerance affect trust, as do previous interactions, shared values, mutual goals, and expressed intentions of the trustee and trusted-other (Holmes & Rempel, 1989). Three types of trust relationships exist in the conceptualization that includes technology: people-with-people (interpersonal; Larzelere & Huston, 1980), people-with-organizations (Mayer, Davis, & Schoorman, 1995), and people-with-technology (Castelfranchi & Tan, 2001). Critical antecedents of technology trust include characteristics of the technology itself, the user, and the task or function (Xu et al., 2014).

People enter into interactions with some initial inclination to trust, but then adjust it based on experience, developing context-specific, learned trust (or distrust; Worchel, 1979). When trust is given and affirmed with positive and beneficial action, the bond is deepened, whereas when trust does not result in beneficial action, the trust bond is reduced, and motives or competence of the trusted-other become suspect (Murray, Holmes, & Collins, 2006). Misplaced or broken trust is seen not as a shortcoming of the truster, but as a failure of the trusted-other (Marsh & Dibben, 2003). In terms of user

performance, trust influences activity, efficiency, productivity, and satisfaction (Cassell & Bickmore, 2003; Kiran & Verbeek, 2010), whereas overtrust results in misuse and error (Xu et al., 2014). In terms of truster *response*, initial lack of trust prevents utilization (Xu et al., 2014), whereas overtrust leads to misuse and disuse (Parasuranan & Riley, 1997).

In business and organizations, trust is essential for organizational success (Rousseau, Sitkin, Burt, & Camerer, 1998). It is facilitated by historical trustworthiness, current competent functioning and accurate communication, and community reputation (Sztompka, 1999). Interpersonal trust is complicated by dynamics of organizational and societal trust processes (Marsh & Dibben, 2003), and individual issues of trust in worksystems are magnified in multiuser contexts, as trust in work-relevant technology affects human communication, work relationships, task performance, and stress (Montague & Chiou, 2014). For organizational and business technologies, when errors occur, the ripple effect of distrust extends out from the interface to the organization it represents (the owner or sponsor) and the organization's leadership (Bahmanziari, Pearson, & Crosby, 2003).

Although these characteristics and processes are derived from dyadic theories of interpersonal relationships, they translate well for contemporary and complex relationships of people (individuals and groups) with technology-based tools and systems (Timmons, Harrison-Paul, & Crosbie, 2008; Xu et al., 2014). The role of trusted-other has been proposed for a range of continuously changing technology components, including user interfaces and information systems, from a human-centric viewpoint framing trust as an ill-structured phenomenon (Marsh, Meech, & Dabbour, 2000; Palmer, Bailey, & Faraj, 2000). The dynamic of trust is premised on the tendency of human users to anthropomorphize technologies, to imbue them with human-like strengths and weaknesses, so they become more than machines, with agent-like identities (Lewis & Weigert, 1985).

One difference between human-to-human trust and human-technology trust is that only the human truster has actual agency, perception, and choice, so conceptualized through agency, trust is functionally static rather than reciprocal (Palmer et al., 2000). On that basis, some studies of technology treat human-computer relationships as static rather than dynamic, and without direct effect on the nature or identity of *either* entity (Kiran & Verbeek, 2010). However, research has demonstrated that trust is dynamic in humans (Vega, Montague, & DeHart, 2011), changing over time based on new information and experience (Zahedi & Song, 2008).

Some studies of e-commerce have focused not on the user-side characteristic of trust, but on the design-side characteristic of trustworthiness (Philosophe, 2000). Others focus on users' responses to interface design esthetics and complexity, rather than the deeper, emotion-charged dynamic of trust (Cassell & Bickmore, 2003). Researchers strive to use trust to predict intended or actual adoption of technology, addressing critical issues for industry (Xu et al., 2014). Although much of this work is still exploratory, trust clearly influences technology use, and technology use presents explicit risks for individuals and society, with ethical implications and life impacts (Hansson, 2009).

Users of websites and digital systems have differential levels of trust based on usability, perceived privacy, and content requirements, all related to purpose (Asan, Perchonok, & Montague, 2012). The construct of trust in websites and e-vendors is composed of externally based perceptions of the vendor (perceived competence, benevolence, and integrity) and the digital system (overall environment safety and specific site quality), along with internally focused willingness (to be vulnerable and take the inherent risk) (McKnight, Choudhury, & Kacmar, 2002). In the digital marketplace of the Internet, distrust resulting from perceived lack of control over information privacy and fear of information and identity theft reduce online purchasing (Araujo & Araujo, 2003). Expensive e-commerce and mobile banking systems remain underutilized, due to trust-related factors (Luarn & Lin, 2005), key components of which are perceived usefulness and perceived risk (Zhou, 2011). Trust of safety and low perceived risk are nonnegotiable in financial systems and those that require disclosure of sensitive personal information (McKnight et al., 2002).

Increasingly, technology is becoming conceptualized as an extension of human beings and human functions (Kiran & Verbeek, 2010), whether used for individual communication, task and activity monitoring, or extensions in the work of skilled technicians. These conceptualizations reach back to the earlier theories of Heidigger (1962) and McLuhan (2001). One complex model of technology trust frames it as interactions of the user's perceptions of the technology (competence, disposition, confidence, dependability, and credibility) and the user's personal tendencies (willingness to persist and complete the task, degree of dependence on the system; Castelfranchi & Tan, 2001). Another model of trust applied to e-commerce frames trust as confidence, based on the credibility of the site source (owner, author, and sponsor) bolstered by authentication (Marsh et al., 2000). Trust leads the user to adopt and commit to use technology, and although there are

many degrees of trust, commitment is more clearly defined. Though a user may look, lurk, and otherwise test a system, a point comes when the choice must be made to trust it enough to utilize it or decline to commit.

TECHNOLOGY, TRUST, AND REDUCED VIGILANCE

In relation to technologies, trust is the degree to which people believe in the veracity or effectiveness of a tool or system to do what it was created for and is purported to do. As a society today, we vest digital technology tools and systems with extensive trust and almost godlike power to control our daily lives and information needs. When they fail, whether due to system glitches or to intentional breaches by others, we suffer a loss of trust. Initial loss of trust is often compounded by further lack of access (through alternate methods) or slow response in remediation or damage control. If the bank's computer goes down, we may have no other way to get at our money; if the Internet goes down, we may have no other way to access the latest news. This lack of alternate access exacerbates people's anxiety and is further compounded by deadlines and risk of loss that will or could result from that system failure. Even new and fragile systems are sometimes trusted as absolutely as systems demonstrated to be more powerful and stable. This blanket trust occurs because many people are ill-equipped to judge the trustworthiness of specific technologies. This inability to discriminate quality in technologies, coupled with the systemic social wave of digitization, leads many people to treat digital tools and systems as a generic whole.

Vigilance, or sustained concentration, is the degree to which people are aware of and monitor the state of a situation, watching for change or signal stimuli (Sternberg, 2009). When individuals believe that someone or something else is watching or monitoring a situation, they become subconsciously less watchful of it themselves; this is the concept of diminished vigilance (Krause & Ruxton, 2002). When people trust digital systems to monitor for error or invasion, to identify threats, they relax their own monitoring, fact-checking, and judgment, relinquishing their decision making to the technology (Hestad, 2001).

ISSUES AND ILLUSTRATIONS

We have all seen or heard about the-document-that-never-arrived, something sent that disappeared into the void while the sender swears to pushing the right buttons and receiving the right feedback from the system. Such events are attributed to every type of tech tool and system, in every kind of organization

and context. When it comes up in a group conversation, the group may be split between those who blame the technology and those who believe the sender goofed and is just saving face. Some such incidents have little effect besides temporary confusion and mild annoyance, whereas others are hugely consequential. In some cases the users' activities can be tracked and even an attempted send verified, but in other cases they cannot, so the truth is never known. The following vignettes are examples illustrating instances and implications of overtrusting technology drawn from: (1) published sources in journals and newspapers, network news stories, and Internet sources; (2) examples shared at IT conferences over the past several years in public presentations; and (3) the author's and colleagues' firsthand experiences.

EXAMPLES IN BUSINESS

Millions of Credit Card Numbers Stolen from Retail Chain

In December 2013, news networks reported that retail giant Target stores' data security system had been breached, resulting in the probable theft of 40 million customers' credit and debit card information (Malcolm, 2014). The information accessed reportedly included not just the individuals' names and card numbers, but also personal identification numbers created as security protection. The breach was not discovered for 3 weeks, during the most active shopping period of the year (November 27-December 15). Target stores trusted its security and monitoring systems, and customers trusted not only the store's technology security but also their banks' and credit card companies' checks and monitoring systems. Yet the networks interviewed victims of theft and losses that left them feeling "robbed" and "violated." Angry customers took to social media to complain and filed lawsuits against the company for "failing" them. Adding to the offense against the wounded, customers could not reach Target stores' customer service to cancel their store cards and avoid additional fraudulent charges (CNN news online, 12/20/13). This very public example of technology overtrust documents the financial, relational, and business risk when trust in a digital record-keeping system is breached, along with the emotional response of customers extending their anger from the system to its sponsor organization, in whom their original trust and high-risk information was vested.

Video Search System

A customer service employee with 2 months on the job in a major video sales and rental company was working with a longtime and loyal customer. The customer asked the employee to order some video packages, but he searched

the database and said the videos were not available and he could not order them. She replied that a different employee told her just weeks ago that they would be available to order by this date, and she had been ordering this series of videos at this store for years. The employee repeated that the system was telling him that they cannot order the videos. The customer asked if there was someone else he could check with, but he replied, "The system shows everything we can get and the system is dependable."

The customer decided to talk to the store manager, who searched a different system and checked the shelf to back up what the technology was telling her. The manager not only found the items but discovered that some were in the store and available that day. Shortly, the customer had her needs met, and her organizational trust was renewed. The manager had to remediate the employee's training and resource-checking procedures—because the employee trusted the initial answer he received from the technology system so much that he not only failed to check an alternative digital source, he didn't even bother to check the shelves. This novice employee's overtrust in a single digital information system caused him to ignore other possible sources of information and nearly cost the store a loyal customer's business.

Prescription Order System

A major chain pharmacy put in a new prescription order system for physicians to place and verify drug orders. The digital system replaced the old, paper-based prescription pads; it was trackable, verifiable, and efficient. One check box in the order interface was whether generic was acceptable, and the default (prechecked) was to allow generics.

One neurologist used the new system to order seizure medication for an epilepsy patient, but did not see the check box to disallow generics. She was continuing a previous prescription with the same patient at the same pharmacy, so she assumed that previous requirements would be observed (trusted the organizational system). However, the pharmacist receiving took the order at face value, filling it as indicated in the digital system (trusted the technology system). The patient didn't notice that what was received was the generic version of the previously brand-name drug she had been taking for years, trusting that the doctor and pharmacist had communicated about her drug needs (trusted the interpersonal professional system). The generic drug did not work for this patient, and she suffered an unexpected onset of seizures, after years of having them completely controlled. When that occurred, the neurologist realized that the drugs received had been the incorrect generic version and tracked the error to the automatic default

in the digital system. The doctor had trusted the new system; her training had not included unchecking the default to generic, and the system design did not clearly cue the need to choose that option. The neurologist also trusted the pharmacy to observe details from past orders of the same drugs for the same patients. The pharmacist trusted the digital system to include any details needed, and the patient trusted that the physician and pharmacist were communicating as needed for her to receive the right drugs. For that patient, the result of all of those levels of trust was a life-threatening error. The error resulted from a series of gaps in communication, each of which pivoted on trust in the design, programming, information accuracy, and checking processes related to the new digital drug-ordering system.

Banking Systems Breached

NBC News broke the story that thousands of banking clients' personal information (including financial information) had been stolen by hackers. In March 2013, news networks revealed that for months hackers had been shutting down online access to the biggest U.S. and international banks (Condon & Craft, 2013). That report included with "relief" that no user money or information appeared to have been taken. As one technologist seeing the report observed in a hallway conversation, "They were just showing off, proving they could control banking access. But if they can shut it down like that, they can get in as well."

In 2014 that prediction came true, as news broke that major banks had again been breached in a series of hackings, and this time customer information had been accessed, affecting millions (Glazer & Yadron, 2014). Customers continued to trust the banks with their money and personal information, even after news of the original bank security breach sparked fear and anxiety. Their continued trust may be due to the perceived integrity and credibility of the banks themselves, as trusted organizations, or to perceived limitations in available alternatives. In a banking network digitally connected, many customers may believe, as one remarked recently, "One bank is about as safe (or unsafe) as another."

Air Travel and Air Traffic Control

One result of overtrust is that people become dependent on technological security and alert systems, to the extent that they are lulled into complacency, taking more risks, and fewer precautions. A tragic early example was in 1988 when the USS *Vincennes* shot down an Iranian airliner, killing 290 people aboard, because the digital warning system identified that plane as hostile

(Hestad, 2001; Wilson, 1988). The person making a decision depended on only one technology-based source of information, a dependency that resulted in the loss of 290 lives. Recent aircraft incidents (such as the mysterious disappearance of Malaysia flight 370) have renewed questions about whether a plethora of alarms and digital monitoring lull pilots and air traffic controllers into diminished vigilance because they expect those systems to alert them when something is amiss (http://en.wikipedia.org/wiki/Malaysia_Airlines_Flight_370). Both the *overreaction* of shooting by the *Vincennes* and the apparent *underreaction* of monitoring Malaysia 370 are examples of reduced vigilance due to overtrust of technology-based systems in high-risk decision making. In each case users apparently depended on technology to the extent of setting aside critical thinking and additional information seeking.

EXAMPLES IN GOVERNMENT

Obamacare Website Rollout Debacle

The entire world is by now familiar with the failure of the US government's national healthcare program online enrollment system in 2013-2014. Out of conflicting reports, assurances, and testimonies to news networks and to the U.S. Senate came the story that the U.S. government had spent billions of dollars on what was supposed to be a sophisticated and secure online healthcare access system, but was overpromised and undertested. The government trusted technology teams to have the system ready, but it was entirely inadequate and chronically dysfunctional. The website failure had massive negative effects on trust in the healthcare system it represented and on the president who championed it (NBC News 11/1/2013).

It was called a "disaster" and a "debacle" on network news, a technology crash that threatened national policy and had a huge impact on political reputation, reverberating up to the Office of the President. The technology system contractors, developers, and overseers were called on the carpet before Congress, and all said essentially that they had done their parts right, but no one appeared to have managed the big picture, including component interfaces. It became a publicly visible example of trusting technology too much in a high-profile, high-risk venture. The ongoing inability of alternative and damage control systems to address emergent needs further alienated intended users. The healthcare website debacle is a stellar example of all three types of trust gone awry (interpersonal, organizational, and technological trust). This complex, dynamic of overtrust cost massively, in time, money, political embarrassment, and anxiety over personal information security.

Associated Press Hack Spread Rumor of White House Bombing

In April 2013 the Associated Press's (AP's) twitter feed was hacked, and a false announcement was spread that the White House had been bombed and the president injured (Domm, 2013). Within minutes the Dow Jones average plunged more than 140 points, and bonds plummeted; though the news was quickly corrected and the market recovered, it was reported that the loss in the S&P 500 index alone cost over $136 billion (Condon & Craft, 2013). Because it carried the credibility of the AP news agency, the original report was absolutely trusted, and people acted on that trust—with profound consequences—without even verifying the report's accuracy. Based on the combination of trust in the media (Twitter) and the purported source (AP), people and organizations reacted in rapid succession and with massive costs before the erroneous message could be corrected. This example also illustrates how damage from technology overtrust is amplified by the speed of twenty-first-century communication.

PERSONAL USER EXAMPLES

Phones as Personal Contact Databases

Recently a friend emailed saying that she needed everyone to send phone numbers and other contact information to her. This end-user had become so dependent on her cell phone that she stopped keeping contact lists elsewhere. When the phone suddenly failed and files couldn't be retrieved, she had to go out and recover them individually. Her lesson learned from this experience was, "from now on I keep an old-school paper list updated as well." Although this example of technology overtrust may seem trivial in comparison to other high-risk examples, it demonstrates that overtrust is not an error of governments or industries alone. Individuals' trust in and dependence on technology tools (computers, phones, and other digital devices) has become absolute. Multiplied by millions of device-users across the United States and around the world, overtrust of personal technology devices that causes people to neglect updating security or backing up information is a serious and potentially life-changing oversight.

Trusting Spelling and Grammar Checkers

We often see evidence that users of word processing systems trust absolutely in spelling and grammar checkers. From errors in business letters and on resumes to uncorrected word usage in academic papers, this nonstrategy

emerges as epidemic. It underscores a pattern of implicit trust that if a word is not flagged as incorrect in a word processing system, then it must be not only spelled correctly but also used correctly. The overarching error is trusting the digital checking system too much, while the underlying functional problem is that such software identifies gross errors (such as nonwords) but cannot discriminate finer nuances of language requiring judgment (like real words used incorrectly). Users from average citizens to business executives have become absolutely comfortable with depending on embedded spelling and grammar checkers that are supposed to autofind, trusting the technology so much that they often do not even proofread. Like overtrust of security monitoring, these personal examples are instances of reduced vigilance due to their implicit belief that the technology is functionally flawless, that if the technology has not found an error, then an error must not exist.

EXAMPLES IN HIGHER EDUCATION

Students Downloading Source Citations

College students in a graduate-level research course downloaded research articles and citations from a library-sponsored national online database, selected the required format, pasted citations into their papers, and submitted them without additional format checking. The citations contained multiple errors (notably punctuation, component ordering, and title case with erroneous capitalizations). Because they were explicitly given responsibility for format correctness, students were marked down on assignment grades. The instructor called the institutional librarian to discuss the errors, and the librarian admitted that errors occurred, and she often heard that students submitted the citations without checking them for accuracy. Because the library had no control over the externally sourced database, her only advice was to continue exhorting students to double-check. This is another example of complex, multiagent trust with cost resulting from gaps in the chain of controls and dependencies. Like the healthcare system, the issue with the academic database is one of many pieces, each with players trusting each other. The university library subscribes to the database and trusts its accuracy, but cannot monitor or control it; given the other benefits, it keeps licensing. Students trust the university and library as sources of accurate research information, so they trust the system the institution sponsors. An effective balance would be to take what the system provides (about 90% accuracy) then check and correct the other 10%, but instead many students accept what is delivered by default, overtrusting the technology system beyond its known effectiveness.

Scheduling on a Digital Calendar

University administrators were puzzled by seeing numerous instances of double-scheduling on their calendars, leading to embarrassing needs to rearrange meetings. An administrative assistant discovered that team and group events entered into the institution-wide calendar tool did not sync up to the server as quickly as they were supposed to, so they did not appear on all attendees' calendars. This meant that others scheduling meetings saw apparently open times where those meetings had already been scheduled. Everyone trusted the calendar tool system to be current and accurate, so they placed events in those "open" times, without double-checking outside the system. Later, when the calendar eventually synced, catching up, the multiple conflicting events appeared. Like the prescription example, this technology system had replaced an older method of phoning or emailing, and users became so trusting of the technology that they no longer checked with the people involved to ensure that the digital information was accurate. A relatively minor error in system functioning—the delay in synching to update meeting schedules—resulted in embarrassment, frustration, and work rescheduling for people who used the digital system to save time and work in the first place. Users who had found the system initially accurate became complacent and trusted it absolutely. A by-product of this overtrust was that missed or double-scheduled meetings were initially blamed on the people involved instead of on the system. Overtrust of the technology resulted in distrust of people as the only other agents in the scheduling dynamic.

University Human Subjects Submission and Processing

A university professor had repeatedly experienced difficulty, error messages, and lost information while using the new institutional human subjects data submission and tracking system. The academic complained to the human subjects office and the technology support unit and was told that he must be making errors, that the system worked fine. After he missed several research opportunities due to the system problems, real glitches were discovered that explained his problems. The administrators working with the system had such absolute faith in the digital technology that they initially assumed user error, rather than digging deeply into the reports, until multiple researchers over time reported the same problems consistently enough. To add to researchers' anxiety, this system was part of an effort to go paperless, so the only copies of forms and documents existed in the system itself—no copy-sent email confirmations, no print-options for users to document

and save their entered information, no alternate methods. This design characteristic implicitly placed absolute trust in the system, and when the system broke, there was no check or recourse for users whose information was corrupted or held hostage. Here as in the calendar example, the trust in the technology—its design, functioning, and information accuracy—were so absolute that technology trust outweighed interpersonal trust. When errors occurred, the people who used the technology were blamed more readily than the technology itself.

Professional Journal Submission System

An academic author entered her information into a digital article submission system, uploaded her documents, and received the message, "Your article has been successfully submitted." After waiting 3 months and hearing nothing, the author emailed an inquiry to the editor, who was surprised and told her that he never saw her paper, nor had any indication that it had been submitted. The editor followed up and found system errors that the publisher corrected over time. Meanwhile, the editor and author facilitated the resubmission of the paper via regular email, and the paper was accepted and published. However, the author's and editor's trust in the system set back that publication more than 6 months beyond the journal's normal submission timeline. This was an instance of disconnect between the users at each end, both of whom trusted information (or noninformation) from the digital system. The author trusted that all was well, based on that message, and waited the 3 months that the journal advertised was its review period. The editor trusted that he was seeing everything submitted to the journal, until he heard from the author, because he had no evidence to the contrary.

Trusting the Cloud

A graduate design class wanted to improve efficiency on student presentations. Instead of each student loading files from individual drives to the classroom presentation system, they loaded them to an Internet-accessible shared storage space. Unfortunately on the day of presentations, classroom Internet access was unavailable. Out of 20 students, only three had brought files backed up on portable media not requiring Internet access. The other 17 had trusted plan A—the institutionally supported Internet access—too much. These students trusted that they would have access to their materials, based on past performance of the system and belief in the university's commitment to ensuring technology supporting their success.

Even Just Email

Due to numerous conflicts and the need to advance schedule, one university started sending out "save the date" emails, up to 6 months ahead of major events. Yet it kept receiving declines and complaints about last-minute notice. Faculty members ignored, missed, or failed to note the "save" dates, while the administrators operated on faith, assuming that the date notices, once sent, were seen and saved. Clearly, they were wrong. Even "read" riders are often inadequate because "read" does not equal "noted" or added to the calendar. The only solution they found was to ramp up "save" to actual "schedule" message, with seamless transfer via direct reply (accept or decline) built into the message, and an event placed on the recipient's calendar. In the original case, the administration had trusted too much, based on implicit assumptions equating different processes of people interacting with digital messages and the interface between two digital systems (email and the calendar), until those assumptions were demonstrated as erroneous. Though the technology technically worked (the emails arrived), the users did not respond as planned, and the administration had overtrusted the effect of the way it chose to communicate, not checking on the response until it was too late and people were double-booked. When they discovered the problem, they upgraded the action role of the technology so it was less dependent on the assumption of human response. Now, however, the entire process was dependent on the accurate functioning of the calendar tool.

Simulations in Medical Education

In the face of time and resource constraints for medical education, much of training and testing for medical specialists such as surgeons is done in simulators, designed as models of relevant human anatomy, often with digital feedback and scoring systems (LeClaire, Nihira, & Hardré, in press). However, these simulators are often designed with less-than-authentic components, and their digital technology systems are limited in the way they score how aspiring surgeons do the work. Some experts and researchers caution against too-ready decision making based on the scores computed by these digital systems, trusting them to determine when a surgeon is ready to operate on real patients (Heinrichs et al., 2007). Trust in simulations for training and development is based on the belief that they authentically train and accurately assess the skills needed. If they do not, then making high-risk decisions based on results from them can constitute overtrust and may have negative consequences. Balancing judgement to err on the

side of caution can be achieved by basing critical decisions on data from more than one source, much like the video store and hostile aircraft examples.

CONTROL ISSUES IN TECHNOLOGY SECURITY

Hacking of technological systems remains an issue for organizations from governments and banks to corporations and professional sports teams. After seeing the movie *Argo*, IT professionals at a conference commented that espionage in the paper age was slower and vastly more secure. When only one copy of a document existed in a warehouse in West Virginia, it could not be accessed from 1600 different digital sites around the world. Shortly after that, news networks broke the story that to help ensure information security, Russia's most secret governmental communication was returning to typewritten documents and storing media without digital archiving (Stanglin, 2013).

International laws and standards also raise issues of control over data storage methods and location. A number of large-scale security breaches have been tracked to overseas databases and blamed on their lack of security, which did not match assurances given to the U.S. companies that contracted them. Similarly, security violations that originate internationally can rarely be charged and adjudicated because of the complexity of international laws and issues of legal domain covering cybercrime. In such cases the administrator (on behalf of users) overtrusts the system's owner or sponsor, failing to fully investigate the security and protections surrounding the system or product being adopted.

MARKETERS PERPETUATING THE MYTH OF TECHNOLOGY INFALLIBILITY

Recently a master's degree graduate in IT went off to invest in an updated home technology system and visited a major national chain store specializing in digital technology systems from business to entertainment. The student shared that she was told the "standard" software "automatically" backed up her data to "the cloud." As a scholar and professional both savvy in technology issues and concerned over data security for confidential client information, she asked a set of questions of the salesperson.

- Whose cloud is that, and what proprietary ownership and access do they retain?

- Where, exactly, is the cloud data stored, and what control do I have over what, when, and how that occurs?
- What options in that agreement can I change, opt out of, or change the defaults on?

The salesperson (though billed as an "expert") had no answers, nor did anyone else in the place. Essentially, he told her that it was "surely" stored safely and "probably" enabled opt-out, but wasn't sure. No buyer control options were specified anywhere in the brochure or information that he could dig up in the store or online. This savvy customer knew what questions to ask and had developed that healthy suspicion that comes from years in the IT field. The average consumer-citizen may not know what to ask and is left operating on faith in the marketers of digital systems. After the student told this story to me, I went to the same company, different store, different salesperson, and asked the same questions. Sure enough, I received similar nonanswers. The salesperson admitted to me that nobody ever asks those questions, that people just accept that "the cloud is a good thing," that they "don't worry about security, like it never occurs to them."

These are the kinds of questions that millions of technology users failed to ask before signing up and entering loads of personal data into Google, only to discover later that their account agreement gave the company the right to mine and sell their data for profit (Tsukayama, 2012).

CAUSES OF OVERTRUST OR BLIND FAITH IN TECHNOLOGY?

Drawing from these and many other examples in the news daily, what can we understand as the causes and characteristics of overtrust in technology?

- General belief in the implicit infallibility of digital technology-based systems.
- Ubiquitous nature of technology in society today, which engenders the belief that there is no other option but digital, so we must accept it.
- Acceptance as ongoing what has been tested or demonstrated initially, failure to go back and check/monitor regularly—expecting success without question.
- Failure to analyze risk implicit and explicit in using digital tools and systems. We don't ask enough "what-if …" questions.
- Assumption that old safety checks and monitoring habits from people-based systems have been carried over consistently to tech-based systems (but too often they have not).
- The people making high-risk decisions (to use, trust, invest in, or roll out these systems) too often do not adequately understand them.

DIMENSIONS OF OVERTRUST IN TECHNOLOGY

The preceding examples illustrate six dimensions of technology overtrust, of three types. Two outcome dimensions are (1) trusting the technology's functionality (trusting that it is working or has worked without thorough testing), and (2) trusting the information that it provides (without alternative sources of verification). Two perspective dimensions are (1) the end-user overtrusting (resulting in lack of backup or alternate access planning), and (2) IT support staff overtrusting (resulting in overlooking possible system errors and tendency to blame the end-user first when complaints are reported). Two critical process dimensions are (1) overtrusting system security (resulting in reduced vigilance, lax monitoring, and delay in catching security breaches, requiring crisis management and damage control), and (2) overtrusting the utility and intuitiveness of user-side features on new digital systems translated from other formats (overlooking nuanced differences with important consequences).

BROAD LOSS OF CONFIDENCE AND GUILT BY ASSOCIATION

With digital technology ubiquitous in society, it is no longer a separate, secret component of business or government, but an inseparable, integrated functional element cutting across systems with which we work every day. As a result, clients, customers, and citizens attribute characteristics of the systems to the owner/sponsoring organization or entity. If the tech system is fallible, then the owner is also fallible by association and may also be judged incompetent, unable to be trusted to do its job well. If technology is insecure so that it creates anxiety and loss of information or resources, then the entity that sponsored it cannot be trusted to protect what is entrusted to it. Thus, the consequences of both overtrust and lack of trust reverberate deeply and broadly. These trust issues also link and are attributed not only to the organization but by association to the people in leadership (e.g., Target Corporation, its CEO; the ObamaCare system, the U.S. government and its president). In this way, the technology tools and systems used by businesses, organizations, and agencies are extensions of these entities. Unlike rogue or criminal employees, due to their nonhuman identity, technology systems cannot be personally blamed. Yet people seek someone to blame for their misfortune, someone with agency to act, so they vest and associate the damage done by failure of technology systems with whomever may be credited with any degree of control.

SUMMARY

In today's globally connected society, business climate, and distributed educational frameworks, digital tools and systems are a central and productive part of communication and workflow management. Much good and useful work and much real backup and protection is made possible with well-tested, frequently monitored, realistically treated and fully understood digital technology tools and systems. However, much loss of money, time, professional integrity, and personal security occurs when people trust technology too much.

We see and hear many examples, shared personally by victims and reported by national and international news services, of tech issues that cost dearly. In some cases these failures could potentially have been prevented. In other cases the failures could not have, but the consequences and costs could have been reduced if someone had possessed more complete knowledge and understanding of the system and its vulnerabilities, or if someone possessing that knowledge had acted on it, rather than trusting the technology too much. A number of factors appear to contribute to this overtrust and reduced vigilance with technology systems. These factors deserve more attention in research and require more attention in the training of both IT professionals and end users.

REFERENCES

Araujo, I., & Araujo, I. (2003). Developing trust in internet commerce. In *Proceedings of the 2003 conference of the Center for Advanced Studies on Collaborative Research. Ontario, CA.*

Asan, O., Perchonok, J., & Montague, E. (2012). Contextual differences in the dynamic measurement of trust in websites. *International Journal of Cyber Society and Education*, *5*(2), 91–110. http://dx.doi.org/10.7903/ijcse.969.

Bahmanziari, T., Pearson, J. M., & Crosby, L. (2003). Is trust important in technology adoption? A policy capturing approach. *Journal of Computer Information Systems*, *43*, 46–54.

Carr, N. (2011). *The shallows: What the internet is doing to our brains.* New York: Norton.

Cassell, C., & Bickmore, T. (2003). Negotiated collusion: Modeling social language and its relationship effects in intelligent agents. *User Modeling and User-Adapted Interaction*, *13*(1–2), 89–132.

Castelfranchi, C., & Tan, Y. (2001). The role of trust and deception in virtual societies. Retrieved from: In *Proceedings of the Hawaii 34th international conference on system sciences*. http://dlib.computer.org/conferen/hiccs/0981/pdf/09817011.pdf.

Condon, B., & Craft, M. (2013). How a false tweet sank stocks. Retrieved from: *MediaWorks*. http://www.3news.co.nz/How-a-false-tweet-sank-stocks/tabid/421/articleID/295530/Default.aspx.

Domm, P. (2013). *False rumor of explosion at White House causes stocks to briefly plunge; AP confirms its Twitter feed was hacked.* CNBC news online. Retrieved from: *http://www.cnbc.com/id/100646197*.

Erikson, E. (1963). *Childhood and society.* New York: Norton.

Fox, A. (1985). *Man mismanagement.* London: Hutchinson.

Glazer, E., & Yadron, D. (2014). JP Morgan says about 76 million households affected by cyber breach. *The Wall Street Journal*. Retrieved from: http://online.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372.

Hansson, S. O. (2009). Risk and safety in technology. In A. Meijers (Ed.), *Philosophy of technology and engineering sciences: 9. Handbook of the philosophy of science* (pp. 1069–1102). Amsterdam: Elsevier.

Hardré, P. L. (2001). Building flexible technology skills using concept models. *Performance Improvement*, *40*(6), 36–40.

Heidigger, M. (1962). *Being and time*. Basil: Blackwell.

Heinrichs, W. L., Lukoff, B., Youngblood, P., Dev, P., Shavelson, R., Hasson, H. M., et al. (2007). Criterion-based training with surgical simulators: Proficiency of experienced surgeons. *JSLS: Journal of the Society of Laparoendoscopic Surgeons/Society of Laparoendoscopic Surgeons*, *11*(3), 273–302.

Hestad, D. R. (2001). A discretionary-mandatory model as applied to network centric warfare and information operations. Unpublished master's thesis. Monterey, CA: Naval Postgraduate School.

Holmes, J. G., & Rempel, J. K. (1989). Trust in close relationships. In C. Hendrick (Ed.), *Close relationships* (pp. 187–220). Thousand Oaks, CA: Sage.

Kiran, A. H., & Verbeek, P. (2010). Trusting ourselves to technology. *Knowledge, Technology, and Policy*, *23*, 409–427. http://dx.doi.org/10.1007/s12130-010-9123-7.

Kramer, R. M., & Carnavale, P. J. (2001). Trust in close relationships. In C. Hendrick (Ed.), *Close relationships* (pp. 431–450). Newbury Park, CA: Sage.

Krause, J., & Ruxton, G. D. (2002). *Living in groups*. Oxford: Oxford University Press.

Krieger, E. (1997). Financing new ventures: A question of trust? In *Paper presented at the 42nd International Council for Small Business World Conference, San Francisco, CA, June 1997*.

Larzelere, R., & Huston, T. (1980). The dyadic trust scale: Towards understanding interpersonal trustin close relationships. *Journal of Marriage and the Family*, *42*, 595–604.

LeClaire, E. L., Nihira, M. L. & Hardré, P. L. (in press). Improving the rigor of validity evidence in gynecologic surgery performance assessment: A critical analysis. *Advances in Health Sciences Education*.

Lewis, J., & Weigert, A. (1985). Trust as a social reality. *Social Forces*, *63*, 967–985.

Luarn, P., & Lin, H. (2005). Toward an understadnign of the behavioral intention to use mobile banking. *Computers in Human Behavior*, *21*(2005), 873–891.

Malcolm, H. (2014). Target breach helps usher in a new world of data security. Retrieved from: *USA Today online*. http://www.usatoday.com/story/money/business/2014/02/22/retail-hacks-security-standards/5257919.

Marsh, S., & Dibben, M. R. (2003). The role of trust in information science and technology. In B. Cronin (Ed.), *Annual review of information science and technology: Vol. 37* (pp. 495–498). Medford, NJ: Information Today.

Marsh, S., Meech, J. F., & Dabbour, A. (2000). Putting trust into e-commerce: One page at a time. In *Proceedings of the fourth international conference on autonomous agents; Workshop on Deception, Fraud and Trust in Agent Societies* (pp. 73–80).

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review*, *20*(3), 709–734.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a website: A trust building model. *Strategic Information Systems*, *11*(2002), 297–323.

McLuhan, M. (2001). *Understanding media: The extensions of a man*. New York: Routledge.

Mikulincer, M. (1998). Attachment working models and the sense of trust: An exploration of interaction goals and affect regulation. *Journal of Personality and Social Psychology*, *74*, 1209–1224.

Montague, E., & Asan, O. (2012). Trust in technology-mediated collaborative health encounters: Constructing trust in passive user interactions with technologies. *Ergonomics*, *55*(7), 752–761.

Montague, E., & Chiou, E. K. (2014). Trust in complex work systems: A focus on information and communication technologies. In C. Korunka & P. Hoonaker (Eds.), *The impact of ICT on quality of working life* (pp. 143–152). Netherlands: Springer. http://dx.doi.org/10.1007/978-94-017-8854-0_9.

Murray, S. L., Holmes, J. G., & Collins, N. L. (2006). Optimizing assurance: The risk regulation system in relationships. *Psychological Bulletin*, *132*, 641–666.

Palmer, J. W., Bailey, J. P., & Faraj, S. (2000). The role of intermediaries in the development of trust on the WWW: The use and prominence of trusted third parties and privacy statements. *Journal of Computer-Mediated Communication*, *5*(3). Retrieved from: http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2000.tb00342.x/full.

Parasuranan, R., & Riley, V. (1997). Humans an automation: Use, misuse, disuse and abuse. *Human Factors: Journal of Human Factors and Ergonomics in Society*, *39*, 230–253.

Philosophe. (2000). *Trust and trustworthiness*. philosophe.com. Retrieved from: http://www.philosophe.com/commerce/trust.html (09.12.01).

Rousseau, D., Sitkin, S., Burt, R., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*, 393–404.

Simpson, J. A. (2007). Psychological foundations of trust. *Current Directions in Psychological Science*, *16*(5), 264–268.

Stanglin, D. (2013). Spooked by NSA, Russia reverts to paper documents. *USA Today*. Retrieved from: http://www.usatoday.com/story/news/world/2013/07/11/russia-spies-nsa-typewriters-documents-computers/2508751/.

Sternberg, R. J. (2009). *Cognitive psychology*. Belmont, CA: Wadsworth Cengage Learning.

Sztompka, P. (1999). *Trust: A sociological theory*. Cambridge, UK: Cambridge University Press.

Timmons, S., Harrison-Paul, R., & Crosbie, B. (2008). How do lay people come to trust the automatic external defibrillator? *Health, Risk & Society*, *10*(3), 207–220.

Tsukayama, H. (2012). Google begins collecting users' data across its services, *Washington Post*. Downloaded 16 July 2013 from: http://www.washingtonpost.com/business/technology/google-begins-collecting-users-data-across-its-services/2012/03/01/gIQAJuXUkR_story.html.

Turkle, S. (2011). *Alone together: Why we expect more from technology and less from each other*. New York: Basic Books.

Vega, L. C., Montague, E., & DeHart, T. (2011). Trust between patients and websites: A review of the literature and derived outcomes from empirical studies. *Health Technology*, *1*(2–4), 71–80. http://dx.doi.org/10.1007/s12553-011-0010-3.

Wehmeyer, K. (2007). Assessing users' attachments to their mobile devices. In *Sixth international conference on the management of mobile business (ICMB), 0-7695-1/07*.

Wikipedia (2014). Malaysia Airlines Flight 370. Downloaded 17 June 2014 from: http://en.wikipedia.org/wiki/Malaysia_Airlines_Flight_370.

Wilson, G. C. (1988). Navy missile downs Iranian jetliner. *Washington Post*, A01.

Worchel, P. (1979). Trust and distrust. In W. G. Austin & P. Worchel (Eds.), *Social psychology of intergroup relations* (pp. 174–187). Monterey, CA: Brooks/Cole.

Xu, J., Kim, L., Deitermann, A., & Montague, E. (2014). How different types of users develop trust in technology: A qualitative analysis of the antecedents of active and passive user trust in a shared technology. *Applied Ergonomics*, *45*, 1495–1503.

Zahedi, F. M., & Song, J. (2008). Dynamics of trust revision: Using health infomediaries. *Journal of Management Information Systems*, *24*(4), 225–248.

Zhou, T. (2011). An empirical examination of initial trust in mobile banking. *Internet Research*, *21*(5), 527–540.