Online Safety in the Age of Artificial Intelligence

NOVEMBER 2019

Family Online Safety Institute

KALEIDO INSIGHTS

About This Report

This whitepaper aims to connect the emerging technological phenomena of artificial intelligence (AI) and its implications with key actions needed to advance a culture of responsibility online. It is not intended to predict the future, but rather to create a basis for discussion among policymakers, law enforcement, industry, academic institutions, parents, and individuals. Its aim is to help identify and prioritize those actions most likely to promote the kind of future that maximizes digital safety while reaping the rewards of technological advancement.

CONSIDER THE FOLLOWING QUESTIONS:

What happens if AI-powered "personal assistants" come to know me or my child better than I do? How will big data influence all of our decision-making?

What happens if bot dependency replaces screens? How can we prepare our children for critical thinking and creativity, rather than over-reliance on technology?

What happens if human-AI collaboration is a job requirement? How will we develop the skills necessary for human-AI partnerships in the jobs of the future?

What happens if we trade tapping for talking? How will using our bodies to interface with devices impact data collection?

What happens if homes get smarter? How can we better safeguard our personal spaces and set a good example for our children?

What happens if everything is gamified? How can we better understand the shifting role of gamification as it integrates with the physical world?

What happens if schools become big children's data hubs? What role will public and educational institutions play in data stewardship?

What is my role in a culture of responsibility? What are the actions and responsibilities of government, law enforcement, industry, parents, educators, and kids? How can we evolve accountability over time?

Introduction

The online safety risks our children face today, such as cyberbullying, predators, sextortion, phishing, and compulsive overuse are a top priority for families. Uncertainty surrounding digital technologies has created new challenges for parents in the ways their children develop and view themselves and the world around them. While parents may reactively try to eliminate risks via heavy-handed restrictions, or by prohibiting their children's use of the Internet altogether, such efforts can deprive kids of an enormous informational, educational, and practical resource.

How must we plan for the future of online safety? The rise of big data has already changed what online safety means. Data is now driving an explosive commercial growth of AI, ushering in a new era of opportunities and risks. We are laying the foundation for software to mimic human qualities, and infuse cognitive capabilities into the objects, infrastructure, and environments that surround us. This whitepaper analyzes the role of AI across both the online and physical world, and examines six research-based forecasts for consideration as we plan for the future of online safety.

In the online world, AI software will define the future of knowledge and decision-making:

1. Empathic computing will increase our reliance on AI
2. AI-powered education technology will scale access to personalized learning
3. The future of work will demand adaptability and human-AI partnerships

In the physical world, AI-powered hardware will transform the interface of the Internet.
As we shift from screens toward machines, they will increasingly read us in return:

1. Our future homes will autonomously sense us and our needs
2. Digital gaming will integrate with the physical world, and across sectors
3. Schools will transform into big children's data hubs

As online and physical worlds converge, **how do we protect, prepare, and project our kids into the future?** First, we analyze what lessons we've learned that can be applied forward. Second, we analyze the need for a cultural shift in how we safeguard technology: from a reactive, siloed approach to a proactive multilateral approach. We must **define a culture of responsibility,** where government, law enforcement, industry, parents, educators, and kids work together.

DEFINITION:
CHILDREN'S ONLINE SAFETY

Children's online safety is often framed in terms of three C's: access and appropriateness of **content**; with whom kids have **contact** online; and how they **conduct** themselves as digital citizens in online communities and as stewards of their own data.

Part I: Artificial Intelligence Permeates our Digital & Physical Worlds

AI has been around for decades, but recent breakthroughs in processing speed, access to big data, and better algorithms have culminated in a proliferation of commercial AI. Online platforms used by billions of people every day use AI to power countless applications from product recommendations to cyber-threat detection, from voice-interactive robots to facial recognition, and far beyond.

Definitions of AI are rarely agreed upon and manifest differently depending on the context. Given the frenetic pace of its development, **AI is best understood as an umbrella term for a variety of methods and tools which mimic cognitive functions across three areas:**

1. Perception/Vision
2. Speech/Language
3. Learning/Analysis

A machine's ability to cognate is supported by multiple approaches – machine learning (ML), deep learning (DL), natural language processing (NLP), computer vision (CV), and many other existing and emerging techniques, multiples of which can be used at the same time for a given use case.

Across these areas, AI is redefining information, and how we interact with digital media.

AI presents a radical shift away from "one-size-fits-all" experiences towards more personalized formats.

The following two sections analyze AI's implications, opportunities, and risks to youth safety across both the online world, extending the web and screen-based applications, as well as the physical world, integrating "digital" to every object and environment around us.

AI AND THE ONLINE WORLD

The vast majority of AI deployed today acts as an extension of digital platforms and software capabilities. While the search, social, and commerce giants are leading in AI adoption and awareness, the reality is we are in the early days of commercial AI.

AI already impacts how we think about children's online safety. For example, both social media and online gaming use AI to promote the most irresistible and influential content. Parental control apps use AI to scan millions of messages sent by children and teens. Industry uses AI to combat the spread of child sexual abuse material through technologies such as Microsoft's PhotoDNA which scans images and videos.[1] AI's accuracy benefits from big data, which presents its own concerns around privacy and targeted advertising to children.

All AI today is "narrow" or "applied AI," which excels at a specific set of tasks. Narrow AI is already providing tremendous value, as it automates countless tasks, optimizes efficiencies, and learns with every interaction. Narrow AI is not without risk, in fact certain risks are accelerated by AI. One example is misinformation, such as deepfake content, a class of synthetic media which, by uploading a selfie, deep learning can cause any child, parent, celebrity, or politician, to do or say anything at all. Forensic tools can hardly keep up, not to mention our ability to discern.

As we all recognize the current opportunities and risks that AI presents to our world, it is important to remember that AI is not magic, it is math: an evolving set of statistical and algorithmic methods. That said, it has profound implications for the future of knowledge and how we make decisions.

NARROW AI

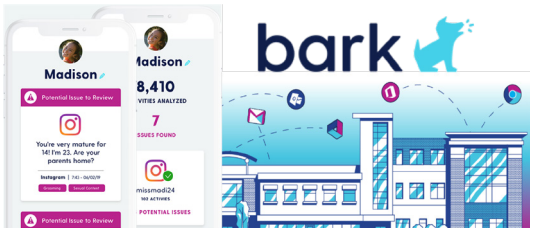

Figure 1: Bark app supports parents and 1,400+ schools with AI-powered risk monitoring. It analyzes all messaging and social media platforms on a child's phone for issues like cyberbullying, explicit content, drug use, depression, dangerous threats, and suicidal thoughts. By only flagging threats when alerting parents or schools, it boasts a "monitoring without snooping" approach, and serves up expert recommendations on how to diffuse specific types of problems, or offer appropriate reassurance when it matters most. Bark claims its technique has prevented 16 school shootings and 10,000 instances of self-harm.

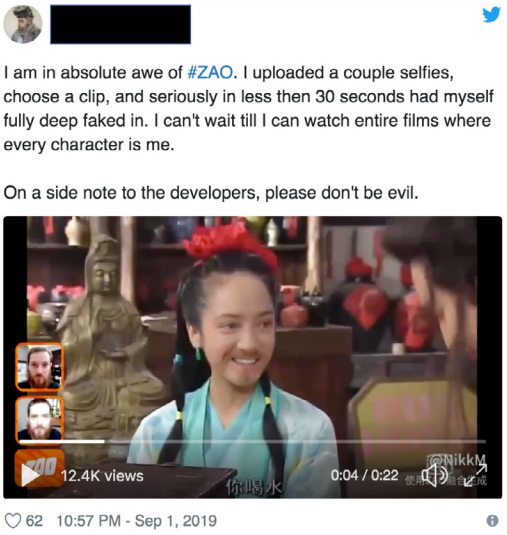

Figure 2: Zao, a recent consumer app using deepfake tech to allow users to upload selfies, their own or others', and superimpose the image on TV clips, movie scenes, memes, or political speeches.

THE FUTURE OF KNOWLEDGE: AI IN LIFE, EDUCATION, AND WORK

From chatbots to personal assistance: empathic computing will increase our reliance on AI

Chatbots are one of the most common applications of AI. These computer programs are able to hold text or audio conversations that convincingly simulate human interaction. Today such conversational agents are found in customer support services, as well as moving from smartphones to speakers, toys, headphones, classrooms, cars, and workplaces. Already, FOSI has found that 23% of American parents have a voice-interactive smart speaker in their home.[2]

In the future, digital assistants will not only pervade our physical world, they will **influence our families' social and emotional worlds too.** Whether a concierge, coach, advocate, or companion, numerous companies are developing technology to respond to this need, with AI-powered humanoid bots that are always available, always learning, and always personalizing.

In the critical years for social and emotional learning, what will be the role of digital companions? Proponents and critics alike emphasize the power of empathic computing, when machines recognize our emotions and respond accordingly.[3] A recent MIT study on the effects of voice-interactive robots and toys found that children aged 6-10 believe that AI assistants are more intelligent than they are.[4] Imagine when these digital companions have years of individualized data, every search, step, and share, every location, handshake, transaction, and breath, as well as **thousands of other data points not even a mother could ever know.**

> ***Will AI-powered "personal assistants" come to know me or my child better than I do?***

AI's growing use of biometric data such as heart rate, sweat, or facial recognition (already collected from millions of devices) can **indicate a wide range of medical, physical, and emotional states.** Even voice data samples offer intimate health information such as fatigue, arousal, intoxication, depression, and diseases.[5]

From standardized testing to personalized education: AI Ed Tech will help scale access to adaptive learning

Teacher shortages and limited funding have historically precluded individualized curricula, but **AI Ed tools are shifting the narrative** away from using highly standardized teaching and learning towards a more individualized and adaptive approach. Tools are evolving towards "intelligent tutoring systems" which adapt daily curricula, instruction, and feedback to students' individual capabilities. Some offer one-to-one tutoring more akin to a human tutor, and even "lifelong learning companions," AI assistants that mentor individuals in and out of the classroom, across all courses, and grades, **continuously developing "21st century" skills.**[6]

> ***How can we prepare ourselves and our children for critical thinking and creativity, rather than over-reliance?***

Many efforts aim not to displace, but help teachers by aiding with or automating tasks like grading, attendance monitoring, lesson planning, translation, and educational data analytics. With growing demands for new types of curricula and wider access to education, AI Ed tools may well be critical to scale educators and widen access to education.

From job-based to skill-based: the future of work will demand adaptability and human-AI partnerships

AI is already impacting the products and processes of every industry, business function, role, and even talent acquisition itself. Although McKinsey and others project AI will displace some 30% of the world's jobs by 2030, **AI won't eliminate, rather it will transform, work itself.**[7] Eight out of ten people expect humans and machines will work together in integrated teams, and numerous studies show that this partnership already outperforms humans and machines alone.[8] **What will partnership look like?** What can educators and parents do to effectively prepare both technological skills and social-emotional skills like empathy, negotiation, and people management?

How will we develop wider skills pipelines for human-AI partnerships in the jobs of the future?

Youth may experience outsized impacts, given the high potential for automation of service jobs such as those in retail or hospitality because they often work in these fields, as Harvard's Berkman-Klein Center points out.[9] Herein lie the risks, not only in reducing youth employment opportunities, but potentially increasing racial, income, and geographic disparities.

Adaptability becomes the essential skill for the shifting occupational landscapes. A 2018 study by the World Economic Forum stated that 54% of the skills that workers need – regardless of industry – will have changed by 2022, suggesting we all should **"skill, re-skill, and re-skill again."**[10] An environment of rapid technological change, organizational agility, and business model change often translates simultaneously to skillset disruption. Although automation may not completely eliminate existing occupations, as it is more likely to replace specific tasks than entire roles, it will shift workers to new tasks, underscoring the need for adaptability.

PERSONAL ASSISTANCE, EDUCATION, WORK

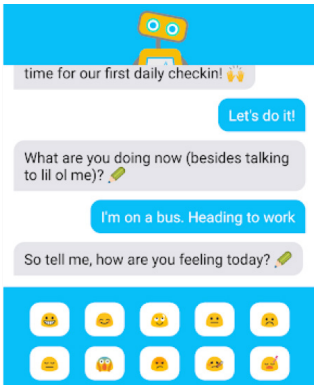

Figure 3: Woebot, a free chatbot therapist available 24/7, offers step-by-step guidance based on Cognitive Behavioral Therapy methods to help users with symptoms of depression, anxiety, relationship problems, procrastination, loneliness, grief, addiction, and pain management.

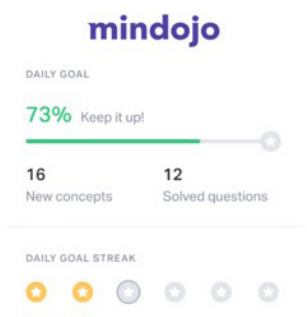

Figure 4: Mindojo, an e-learning platform that develops algorithms to "learn the learner." By analyzing the timing, text, and context of each student answer, Mindojo over time develops a specific curricula most suitable to each individual's cognitive and emotional strengths, weaknesses, and personality type.

Figure 5: AI Goes to Work: From drone-powered safety monitoring of construction sites, to biomarker recognition consulted for medical diagnostics, from automated prospect profiling for sales agents, to deep learning-powered design simulations for manufacturing, applications in worker augmentation and job displacement abound.[11]

AI AND THE PHYSICAL WORLD

What was once a clear distinction between online and offline is blurring. Embedded sensors connect and integrate "things," objects, animals, plants, people, devices, machines, infrastructure, and environments, to information networks. **The Internet of Things (IoT) is an all-encompassing term for the interconnectivity of digital and physical worlds.** Increasingly, AI software is finding its way into IoT hardware and sensors, integrating with all manner of devices with perception, linguistic understanding, and learning capabilities.

There are already many more billions of IoT connected devices than humans on the planet, and this number is estimated to reach over 34 billion within the next five years.[12]

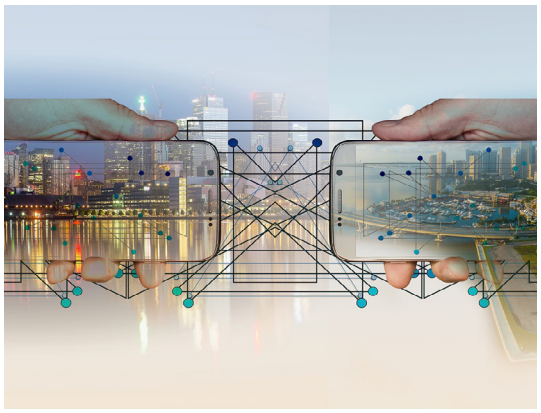

Figure 6: The Internet of Things connects digital to physical

Safety is one of the top selling points for IoT devices in the smart home market.[13] Although the term IoT is not widely recognized by parents, a 2017 study by FOSI found that 45% of parents indicate their child has 3 or more IoT devices of their own.[14] Parents are using smart watches or mini-phones like the Palm to geo-track their children. Caregivers and doctors are using cameras, wearables, and even pill containers outfitted with sensors and computer vision to analyze biometrics and movement. Countless **dangerous jobs** are better managed by AI and IoT-powered machines or robots, not to mention the employee safety implications of smart helmets, wearables, and smart cameras to prevent injury, overexertion, and hazardous conditions. Safety is only the beginning. Smart infrastructure will grow more ubiquitous because **organizations view IoT and AI as critical enablers** to optimize product performance, maintenance and energy efficiencies, customer relationships, and data for business model innovation.

IoT also opens up new vulnerabilities. Devices, routers, and networks are now **targets for nefarious data breaches,** identity theft, even overriding home controls or locks. Devices may also **collect vast amounts of personal data,** adding to concerns around privacy and data abuse.

As we add AI sensors to every *object*, we aren't just integrating data streams and cognitive features into our world. **We're transforming the very interface of the Internet.** Shifting away from screens and text-based interactions means our devices will read us, our eyes, expressions, movements, and biometrics. Today we're **talking and gesturing** with our devices. Soon headsets will **augment our sight and hearing,** superimposed with digital content. Auto manufacturers are developing dashboards with **facial recognition** to detect fatigue, and retailers are investing in **smart mirrors** to discern customer sentiments.[15] Imagine how instead of keys, credit cards, or passports, we will use **biometric authentication,** our faces and fingerprints, to access our homes, authenticate payment, or go through airport security.

How will using our bodies to interface with devices impact which data are collected?

This convergence will render **interfaces invisible.** Amazon Go, the frictionless grocery store that eliminates the checkout experience allows shoppers to walk in, pick their desired items from the shelf, and simply walk out. The experience for shoppers *feels* largely tech-free, despite a complex technological configuration across sensors, hardware, and software.

IOT & COGNITIVE DEVICES

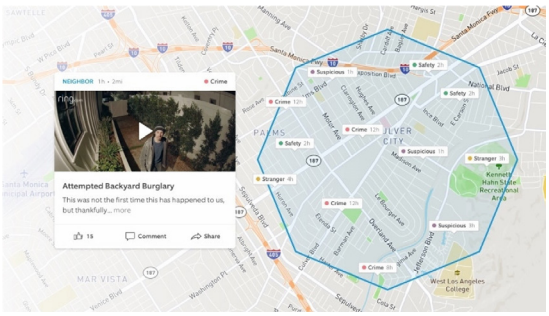

Figure 7: Amazon's Ring Doorbell and Neighbors App: Amazon's Ring Doorbell system is more than a connected doorbell and CV-enabled camera for answering the door from anywhere, its accompanying Neighbors app is a platform for real-time crime and safety alerts from neighbors integrated with local law enforcement.

Figure 8: CloudToys paid the price for weak security when its "smart" toys were removed from the shelves of Amazon, Target, and Walmart in 2018, after extensive security threats were uncovered, compromising some 820,000 records including children's names, ages, and voice recordings.[16]

THE FUTURE OF INTERFACE: AI IN THE HOME, GAMES, AND SCHOOLS

From disconnected homes to ambient computing environments: Future homes will autonomously sense us and our needs

Just about everything in the home, from lightbulbs to baby monitors, is **increasingly interconnected and AI-enabled.** Smart toys are already found in one of three homes, from stuffed animals to toy cars to robots, offering kids interactive and immersive stimulation and echoing previous generations' make-believe.[17] Smart toys are outfitted with sensors, microphones, cameras, and software to enable personalized responses and experiences in real-time. Some "learning" toys are even **programmed to teach kids skills** like coding, drawing, math, or language, and have been found to **improve communication skills** particularly among children with intellectual disabilities.[18] But these toys can also jeopardize safety and privacy, as they often face security challenges and can be used to access other data and devices on the network.[19]

How can we better safeguard our personal spaces and set a good example?

Home isn't just the entry point for kids' use of technology, it is also the **critical domain for parents to model good behavior** in how they use and safeguard devices. The smart home ecosystem, from Google to Whirlpool, isn't working towards a future of products, but towards a future of services enabled by ambient computing.[20] Instead of humans seeking information from devices, embedded sensors and software will autonomously sense, recognize context, and adapt **anticipating our needs and protections without conscious mediation.**

From online games to real-world economies: Digital gaming will merge with the physical world, across sectors

Over the last decade, the astronomical growth of software games, e-sports, mobile apps, and massive multiplayer online games have raised hundreds of billions of dollars, influenced tech designs, and created passionate global communities. **For some, gaming is the first entry point for technology.** A recent study found that girls who play video games are three times more likely to pursue a STEM degree.[21] Today some 30% of the world's population are active gamers.[22]

The future of gaming may be even more influential, particularly as it integrates with the physical world and across sectors. Its parallel development with AI and IoT will unleash augmented and virtual gaming overlaid with real-world environments. Games are already beginning to collect location, fitness, weather, or other sensor data, but imagine how immersive games will feel when biometrics and emotional data feed algorithms to dictate the intensity of the course and competition. Imagine further how AR gaming could incentivize real world actions, for example to improve efficiency or promote healthy decisions, and compensate those actions with digital coins that are interchangeable across an ecosystem of partners. After all, **microtransactions and accumulation of virtual wealth** based on in-game achievements and economies are already ubiquitous in gaming, and may accelerate gamification across sectors.

From "dumb" buildings to cognitive infrastructure: schools will transform into big children's data hubs

Sensors, cameras, and connected infrastructure are also infusing our public spaces, from city sidewalks and parks to museums and schools. Although different schools have different policies around tablets and mobile devices, **AI-powered infrastructure will inevitably become part of school campuses.** Already, schools are using smart cameras to surveil the environment and identify unauthorized persons, employing smart lighting and HVAC systems for energy efficiencies, and installing smart locking systems.

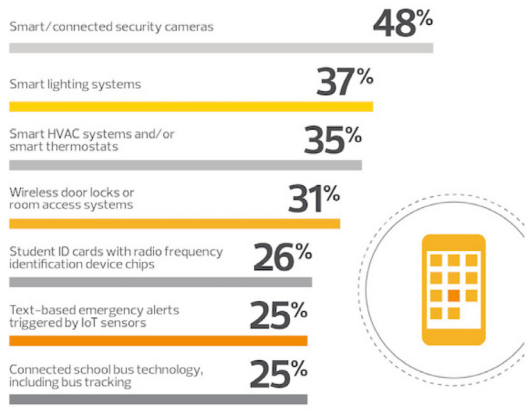

Figure 9: IoT Deployments in Schools, via CDW

What role will public and educational institutions play in data stewardship?

Schools' **adoption of IoT is particularly relevant to youth safety because it catalyzes the volume and variety of data collected.** A recent CDW study found K-12 decision-makers are evaluating IoT tools to improve campus safety and student engagement, and to drive efficiencies and cost reductions.[23] While the CDW study found 81% of respondents feel the potential benefits of IoT in K-12 will outweigh the risks, this tension is put to the test every day.

Should schoolwork count toward the hours of screen time kids spend per day? As AI tools ask questions and monitor students' mental health, how can we prevent unauthorized use or "scope creep" of this data? Should schools monitor kids' individual social media accounts and activities? Should that data be stored and for how long? Should it be shared with law enforcement? **What is the role of ubiquitous sensing and big data in protecting kids from modern day risks?**[24]

HOME, GAMES, SCHOOLS

Mattel's AI-enabled Hot Wheels™ id lets kids compete both physically with an IoT racetrack and virtually using an augmented reality (AR) app.

KindVR works with healthcare providers to mitigate pain and ease tension involved in certain medical and pediatric procedures. VR and AR are cropping up in tourism, HR programs, to raise awareness (and dollars) for charities, and for more efficient training across every industry.[25]

School bus-tracking apps help parents and kids coordinate timing, simultaneously offering fleet managers the ability to monitor driving and predict maintenance.

Part 2: Opportunities & Risks AI Presents to the Future of Family Online Safety

AI presents powerful opportunities and risks to online safety. Below we chart examples of each, and key trends to watch over the coming years.

	OPPORTUNITIES	RISKS
AI in Personal Assistance *Empathic computing will increase our reliance on AI*	• **Personalized decision-making** and risk assessment, based on real-time personal data and context • **On-demand and accessible to all:** Increasingly across any app ecosystem and device • **Beyond human assessment:** Big data inputs enable analysis across thousands of dynamic factors, from health to history to real-time environment	• **Security and privacy:** All software can be hacked, manipulated, exploited • **Erosion of agency:** Emotional manipulation, over-dependence on software-powered guidance • **Commercially developed:** AI may prioritize business model over wellbeing metrics or human-human interactions • **Duty to report:** If child-AI dialogue reports self-harm, crime, or abuse, who has a duty to report?
AI in Education *AI Ed Tech will scale access to personalized learning*	• **Scales access to educational resources:** Supports individual learning styles and reduces achievement gaps • **Dynamic education:** AI Ed tools always-on, more efficient to program, always learning as 21st century skills rapidly shift • **One-to-one interaction:** Frees up teachers for face-to-face engagement and more social and emotional learning • **AI Ed for AI engagement:** Tools could be used to build kids' AI fluency, train on AI design, ethics, bias, transparency, etc.	• **Quality content:** AI Ed does not create quality content, metrics, or courses; requires educator training and expertise • **Security and privacy:** How to safeguard sensitive student data, prevent advertiser profiling, future abuse/exploitation • **Hyper-personalization could erode collective** experiences/cohesion among youth, appreciation of diverse sociocultural backgrounds • **Undermines "offline" education:** if personalized education requires high tech, what about other life skills?
AI in Work *The future of work will demand adaptability and human-AI partnerships*	• **Humans can avoid dangerous jobs:** Robotics/AI deployed in high-risk environments • **Human-machine partnerships:** May perform better and safer than either alone • **Augmented adaptability:** Tools could be used to exercise critical skills training, around safety and beyond	• **Lack of diversity:** Automation risks outsized impact on underrepresented groups, exacerbating employment and wealth gap • **Skills pipeline accelerating:** Cannot keep up with shifting occupational demands, including safety and governance automation oversight • **Fulfillment and purpose:** Eroded through automation, job displacement; social safety net cannot bear rising unemployment

AI & IoT in the Home *Our homes will autonomously sense us and our needs*	• **Stronger security:** "Smart" cameras and security systems safeguard individuals and support neighborhood watch • **Stronger parental controls:** Tools are offering more sophisticated controls and multi-user experiences, out of the box • **Smart homes:** Home is a microcosm of connected devices that present opportunities for teachable moments	• **Security and privacy:** Devices can be hacked, biometric and other data exploited, physical systems and users manipulated • **Interconnected does not equal secure:** More sensors and software integrated throughout home life introduce new vulnerabilities • **Parents as IT admins:** Some parents are not aware, nor equipped, to monitor/ mitigate diverse digital challenges at home
AI & IoT in Gaming *Digital gaming will merge with the physical world*	• **Educational opportunities:** Gaming is a prime platform for learning, modeling conduct, content, contact, privacy protection • **Improves access:** Gaming offers opportunities across all learning types and backgrounds • **Games for resilience:** Virtual environments help build empathy, troubleshooting, leadership, and economics	• **Unwanted contact:** Virtual environments can have trolls, bullies, predators, voyeurs, or other inappropriate or illegal actors • **Nefarious tools:** Bad actors have diverse toolkits, from chat to cameras, hacking to voice-masking • **Social isolation:** Parents should model good time management and explain restrictions
AI & IoT in Schools *Schools will transform into big children's data hubs*	• **Improved physical safety:** Cameras, big data, smart locks, multi-device alerts, and ID authentication have thwarted attackers • **Improved harm prevention:** Real-time sensing identifies risk and alerts educators and triggers preventative measures • **Improved online safety:** Clear guidelines, common curricula improve teacher, parent, and student understanding and instill stronger digital citizenship	• **Privacy consequences:** Schools have uniquely intimate, multi-domain, and long-term data collection potential for youth. They must consider good data practices so as not to harm students • **IoT security risks:** Vast scope and size of campuses, devices, users, and turnover requires significant security resource investment • **Increased disenfranchisement:** New technologies are expensive, performance and security require reliable connectivity unavailable to low-income or rural districts.

KEY TRENDS TO WATCH

- AI handles more decision-making
- Empathic computing
- Increased data collection
- Voice displaces touch/tap
- Ambient computing
- Virtual currencies
- Growing digital divide
- Schools' use of big data
- Digital citizenship

Part 3: Six Generational Lessons for the Future of Kids' Online Safety

Part of preparing for AI's impact on online safety requires we analyze the existing wisdom that we can apply. What follows is a summary of takeaways from interviews and analysis across parents, grandparents, teachers, librarians, and cyber safety experts.

LESSON #1: MODEL GOOD BEHAVIOR.

The most evergreen advice of all: set a good example. As in most realms of development, parents set foundational templates for navigating the world, problem-solving, and relationships. Technology is no different. Across interviews, parents acknowledge two points:

1. Parents admit they themselves aren't always the best role models for online safety, conduct, content, screen time, privacy and security settings
2. Kids are more perceptive, intuitive, and attentive than we may want to believe

Here the 3 C's of online safety, content, contact, conduct, serve as a strong framework, but good behavior will also evolve alongside kids and tech. Teens will observe and act on parents' online examples differently than toddlers. Advice from a pre-smartphone era 10 years ago may sound quaint by today's standards, and so it will be 10 years in the future. This underscores the need to start the conversation early, and keep it going.

"To teach my son empathy and communication, I have to be the one to turn off the 100 million notifications, to show him what it looks like to be in control of my time and attention. This is one of the best gifts we can give our kids."

– Mother, Georgia

Key takeaway: Adults' digital citizenship informs kids' behavior. View your own good choices not only as day-to-day cues, but as strategies for demonstrating critical thinking and responsible behaviors that align with your family's values.

LESSON #2: PARENTAL STRATEGIES MAY DIFFER.

How parents approach kids' use of technology differs widely. From helicopter parents to hands-off parents, approaches to kids' online safety varies from restrictive to permissive. Parents with a conservative approach to tech may limit kids' screen use strictly, whereas more lenient parents may trust their kids to make their own tech decisions. It is important for parents to maintain a balanced approach to preparing kids, both questioning future tech implications and recognizing that tech will be pervasive in their lives.

"How parents address these choices constitutes the great parenting divide of our time… A divide over how kids use of technology shapes family life and future prospects has far-reaching impacts."

– Alexandra Samuel, digital parenting expert

Key takeaway: Spend time online together, acknowledge that everyone makes mistakes, establish an ongoing dialogue about technology, and aim to build trust and mentorship at every age to prepare responsible digital citizens.[26]

LESSON #3: BE PROACTIVE.

Parents and caregivers must now guide children towards adulthood in a world increasingly unlike the one they grew up in. Across the board, parents interviewed place the responsibility on themselves, but this requires a proactive approach to understanding the opportunities and risks of technology.

"Right now you have some parents asking why you haven't put your kid in coding classes, and other parents decrying any screen time at all!"

– Father, California

Key takeaway: Parents must educate themselves. Commit to some degree of ongoing tech awareness or education, such as attending a parenting seminar or PTA workshop, seeking materials from reputable sources, or learning a new skill or game alongside kids.

LESSON #4: EXERCISE ANALOGOUS THINKING.

Parents need to look no further than their own childhood experiences to better sympathize and understand kids' relationship to technology. The concerns the previous parental generations may have had around analogous media consumption are still applicable to parental concerns today.

There are fundamental differences here between previous forms of media and the Internet, particularly around data collection, sharing, and the potential for exploitation. But there are also important similarities, which can be instrumental in developing parents' empathy, forecasting risks, and remaining open when kids share their stories, and most importantly, when building ongoing trust and rapport.

Key takeaway: Identify an analogue of similar games, toys, relationships, or events that emerged through your own childhood, and leverage these in times of tension or teaching.

LESSON #5: MINIMIZE KIDS' DATA DEBT.

Few parents today are aware that many online platforms and connected devices are collecting, sharing, and monetizing data, which is then used for profiling. The question of whether commercial actors, advertisers, and data brokers harvest kids' data has many implications. Even beyond how such data are often used today, often for behavioral marketing, do we really want kids' personal data trails to impact their future opportunities, such as college admissions or loan approvals? What about for kids with limited access to technology? For kids with behavioral or developmental issues? How can our online safety decisions today prevent imposing a data debt on future generations? Parents and educators play a critical role here at home and school, as the primary purchasers of the products and services harvesting such data.

"When you're engaged in service delivery to children, the bar for data use should be high, and it's not today. Moreover, kids at the bottom of the social ladder are impacted first. We can do better."

– Teacher, Washington, DC

Key takeaway: Parents and educators must aim to understand how platform providers collect kids' data, exercise discretion, align with other parents and school administrators, and appeal to local leaders.

LESSON #6: IT TAKES A VILLAGE.

Many stress the need for more accountability, support, and collaboration. This is needed not only to safeguard our online and physical worlds, but certain elements of the human experience: empathy, respect, discernment, adversity, and resilience.

"How we engage around technology, how to ensure divergent thought, how to really make sure this is safe for our kids… this is all of our responsibility. We can't let our increased dependency on tech erode our humanism. Instead we should imbue our humanism into tech!"
– Grandfather, California

Part 4: Societal Forces

As deeply and widely impactful as they may seem, the key technological trends outlined above do not exist in a vacuum. First, AI and IoT are not the only technology shows in town; from connected cars to 5G connectivity to cryptocurrencies, advancements and **convergence are occurring across every part of the technology stack.** Second, all of the above impact industry in distinct ways, all forecasting different futures.

The future will always be an **unpredictable amalgam** of cultural, political, economic, and environmental forces. Cultural forces and tensions vary dramatically across regions, but always inform our decisions and differences. Political dynamics and government structures influence strategic priorities, access to resources and capital, and set the framework for multilateral collaboration. Our modern economic engine, enmeshed globally but experienced locally, is the great shared exchange in which we all participate. Our environment literally provides the resources and context for all of the above. As we plan for the future of online safety, we must plan for this changing, dynamic, increasingly interconnected, multilateral, and systemic reality. These unpredictable fluxes only underscore the need for a culture of responsibility.

SOCIETAL FORCES & THE RISE OF CAR-SHARING

Few predicted the rise of car-sharing tech companies like Uber and Lyft. Even fewer consider this global disruption the result of 4G cellular networks, cloud computing, smartphone reliability, real-time sensors, and localization technology. Somehow, the cultural preference for access over ownership and convenience over concern prevailed over the old "never get into cars with strangers" dictum. Culture, after all, informs how we define "safety" and weigh the risks. Such apps have disrupted multiple industries and ushered in an altogether new "sharing economy" infrastructure that mobilizes millions of people, reduces carbon emissions and is currently valued at more than $300 billion.[27] These changes have also been met with a waterfall of government responses, regulatory questions, and lawsuits.

Part 5: Implications for a Culture of Responsibility in the Future

Our online and physical worlds are converging, and so must our sense of accountability. As AI and ubiquitous sensing interconnect everything around us, online safety becomes a shared priority. **It is imperative we work to institute a culture of responsibility now,** in what are no doubt the earliest days of these technologies' applications, risks, and societal integration.

Perhaps the most imminent question amidst so much technological disruption is who controls, designs, regulates, and benefits? How can we reap and share the profound rewards these powerful tools offer, while mitigating equally significant potentials for abuse? Here the spirit of a culture of responsibility is most important: **everyone must play a role** in how we use technologies to enhance and extend the health, wellbeing, civil liberties, and safety of individuals and society as a whole.

Based on our ongoing scrutiny of emerging technology trends, analysis of each stakeholder group, and current examples of responsible technology stewardship, we propose the following key actions as the basis for a culture of responsibility.

KEY ACTIONS FOR A CULTURE OF RESPONSIBILITY					
Government	**Law Enforcement**	**Industry**	**Parents**	**Educators**	**Kids**
Develop comprehensive national strategy for disruptive technologies and AI Institute reasonable government oversight grounded in research Dedicate full-time roles and resources for online safety	Enhance resources across agencies Establish consistent education and training Facilitate collaboration and trust	Pursue robust and comprehensive self-regulation Institute collaborative structures to foster safety Prioritize safety through design and metrics	Model responsible behaviors of good digital citizenship Communicate and participate with kids Seek guidance and resources	Equip with consistent education guidelines Provide resources to bridge the gap(s) Employ dedicated roles and resources to preserve school safety	Involve youth in co-creating the future Exercise good digital citizenship Foster resilience
MULTILATERAL APPROACH | EVIDENCE-BASED, NOT FEAR-BASED | CLEAR COMMUNICATION ACCESSIBLE GUIDANCE | ADAPTABLE AS TECHNOLOGY EVOLVES					

GOVERNMENT

1. **Develop a coherent and comprehensive national strategy for disruptive technologies and AI.**
   Government defines strategic goals, key metrics, and scope of governance standards for security, wellbeing, risk mitigation, and multilateral engagement.
2. **Institute reasonable government oversight grounded in research.**
   Rapidly advancing technologies and predictive automation call for legislative efforts to shift from reactive towards more proactive and evidence-based. Dedicated funding for ongoing policy research on impacts of emerging technologies on family safety in areas of health, education, and media.
3. **Dedicate full-time roles and resources for online safety.**
   As an example, a new role, Chief Online Safety Officer for the United States, works alongside the US Chief Technology Officer to coordinate online safety across agencies and departments, convene leaders in industry, non-profit, and academia, and advise resource allocation supporting the evolution of online safety.

LAW ENFORCEMENT

1. **Enhance resources across agencies.**
   To combat the growing velocity and variety of threat types, enforcement officers and agencies are equipped with state-of-the-art tools, techniques, best practices, and support to deter crime and identify opportunities to better protect and organize for safety.
2. **Establish consistent education and training.**
   Implement a comprehensive curricula to include clear standards, guidelines, and processes, informing how law enforcement agencies approach cybercrime. Training includes approaches to combat nefarious use, big data abuse, crowdsourced threats, AI ethics and design, communications, and other emerging risks.
3. **Facilitate collaboration and trust.**
   An essential line of defense for online safety, law enforcement collaborates with industry, academic institutions, and communities to thwart attacks, investigate crime, expedite safeguards, and foster trust.

INDUSTRY

1. **Pursue robust and comprehensive self-regulation.**
   Digital innovations are coupled with forward-thinking self-regulatory efforts and investment, including policies, practices, designs, audits, and dedicated resources that protect users, encourage positive behavior and user wellbeing, and preserve civil liberties. Governance must also "think global, act local," keeping pace with increasing scale of operations domestically and internationally.
2. **Institute collaborative structures to foster safety.**
   It is imperative that organizations, and especially technology companies, collaborate with one another to reduce online safety risks, conduct risk/benefit analyses, and to prevent unintended consequences.
3. **Prioritize safety through design and metrics.**
   Protections, controls, and efficiencies are engineered into product and services "by design." Performance metrics should also prioritize user safety, security, and community health.

PARENTS

1. **Model responsible behaviors and good digital citizenship.**
   Like many behaviors, parents also set the template for digital citizenship and safe digital practice. Model respectful conduct, provide safety guidance around digital contact, exercise discernment in content and your own digital footprint and reputation, and demand clarity from service providers. Help kids develop their own resilience.
2. **Communicate and participate with kids.**
   Guide kids' digital journeys, starting from an early age. Communicate directly about their online activities, favorite games, channels, devices, and engage in both enjoyable and teachable moments. Equally important is demonstrating parents' own proficiency, boundaries, common sense, and the joys of being on and offline.
3. **Seek guidance and resources.**
   Technology is constantly changing, but parenting always requires preparation. Solicit advice, engage in dialogue, find tools, and resources from other parents, PTAs, teachers, school directors, community leaders, and reputable online sources. Remember, tactics and solutions will continue to evolve right alongside technologies and risks.

EDUCATORS

1. **Equip with consistent education guidelines and tools.**
   Educators are provided with comprehensive and research-based curricula to teach digital citizenship and technology ethics and design across multiple grades and course domains. Clear guidelines and tools also support student exercises, issue-resolution, parental collaboration, and use of AI Ed tools.
2. **Provide resources to bridge the gap(s).**
   Schools play an essential role in developing a diversity of skills pipelines and bridging achievement gaps. Ensuring funding and access to resources is essential to encourage children from minority, rural, or other underrepresented populations to explore and develop the skills of the future and participate in and pursue opportunities harnessing emerging technologies.
3. **Employ dedicated roles and resources to preserve school safety.**
   School districts benefit from a dedicated online safety office focused on balancing positive technology use in education with IT departments to adhere to rigorous data and systems security standards that prioritize student and campus safety.

KIDS

1. **Involve youth in co-creating the future.**
   Youth of all ages and backgrounds are empowered to contribute to discussions, decisions, and designs of what the future of technology looks like. Industry, parents, teachers, and community programs foster dialogue, hackathons, DIY challenges, and other forums for co-creation.
2. **Exercise good digital citizenship.**
   From an early age, kids are taught to take the rights and responsibilities of online safety seriously. Industry, parents, teachers, and community work together to reinforce good digital citizenship as kids, and technology evolve.
3. **Foster resilience.**
   Regardless of age, the most essential ingredient for good digital citizenship is resilience. Adversity and consequences happen in life, online and offline, and adaptability is key.

Part 6: Conclusion

If you want to go fast, go alone. If you want to go far, go together.

As tools evolve, so too will opportunities and challenges for online and physical safety. A dynamic and modern world requires adaptability and resilience for individuals and organizations alike. The culture around technology today is often about speed and advancing as quickly as possible, but as technology integrates with every part of our world, including ourselves, we are all navigating uncharted territory. From leaders to lawmakers, parents to police officers, doctors to designers, teachers to teenagers, we all have a role in shaping adoption and governance of our future technologies.

METHODOLOGY

This report was produced as a result of analysis conducted by Kaleido Insights, and developed on behalf of the Family Online Safety Institute between August and October 2019. The trends and analysis included in this report were synthesized from a multi-modal set of research inputs Kaleido analysts reviewed, including research interviews, reports, commercial activity, conferences, client work, and secondary research.

INTERVIEWS

- Alexandra Samuel, Ph.D, Journalist, Digital Parenting Expert
- Tatiana Jordan, CMO at Bark
- Lauren Harper, Director of Marketing at Palm
- David Harley, Former Sr. Research Fellow at ESET NA
- Teacher, California
- Teacher, Washington D.C.
- Librarian, California
- Mother, British Columbia
- Mother, Indiana
- Mother, Georgia
- Father, Virginia
- Mother, Alabama
- Mother, Iowa
- Father, California
- Grandfather, California
- Engagement with Wall Street Journal's "Parenting in the Age of Tech" Facebook Group

ABOUT THE FAMILY ONLINE SAFETY INSTITUTE

The Family Online Safety Institute is an international, non-profit organization that works to make the online world safer for kids and their families. FOSI convenes leaders in industry, government and the non-profit sectors to collaborate and innovate new solutions and policies in the field of online safety. Through research, resources, events and special projects, FOSI promotes a culture of responsibility online and encourages a sense of digital citizenship for all. FOSI's membership includes 20+ of the leading Internet and telecommunications companies around the world.

ABOUT KALEIDO INSIGHTS

Kaleido Insights is a research and advisory firm focused on the impacts of emerging technologies on humans, organizations, and ecosystems. Our mission is to enable organizations to decipher, foresee, and act on technological disruption with agility. Kaleido's analysts support clients with a research-based approach to digital transformation strategy development, as well as forward-looking original research, trends analysis, use case evaluation, and market leadership advisory.

ABOUT THE AUTHOR

Jessica Groopman is an industry analyst and founding partner at Kaleido Insights, where she leads the automation practice and specializes in AI, blockchain, IoT and cultural dynamics influencing adoption. Jessica is a frequent speaker at emerging tech industry events and a regular contributor to numerous media outlets and trade publications. She has been principal analyst with Tractica, Harbor Research, and Altimeter Group and has served as a contributing member of the International IoT Council, the IEEE's Internet of Things Group, the DigiGuru Network, and was included in Onalytica's list of the 100 Most Influential Thought Leaders in IoT. Before she worked in business and tech research, Jessica's research experience was based mostly in academic anthropological fieldwork, specifically in ethnographic, linguistic, and archaeological research both in the United States and abroad.

ENDNOTES & REFERENCES

[1] Langston, Jennifer. "How PhotoDNA for Video is being used to fight online child exploitation" *Microsoft On the Issues Blog*. 2018, Sept. 12. Accessed 2019, Sept. 14. https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-video-is-being-used-to-fight-online-child-exploitation/

[2] Survey of 601 parents and qualitative focus groups to determine parents' perceptions of wearables, toys and IoT. "Connected Families: How Parents Think & Feel about Wearables, Toys, and the Internet of Things" Family Online Safety Institute & Hart Research. 2017. Accessed 2019, Aug. 17. https://www.fosi.org/policy-research/connected-families/

[3] **Empathic computing** is category of computing systems and devices which aim to recognize, understand, and process human emotions and states, simulate them and interact accordingly; Affective computing or artificial emotional intelligence is a subset which uses machine learning, computer vision, and other AI techniques.

Billinghurst, Mark. "The Coming Age of Empathic Computing" Medium. 2017, May 4. Accessed 2019, Sept. 14. https://medium.com/super-ventures-blog/the-coming-age-of-empathic-computing-617caefc7016

[4] Druga, Stefania and Randi Williams. "Kids, AI devices, and intelligent toys" MIT Media Lab. 2017, June 6. Accessed 2019, Sept. 11. https://www.media.mit.edu/posts/kids-ai-devices/

[5] Mullin, Emily. "Voice analysis tech could diagnose disease" *MIT Technology Review*. 2017, Jan. 19. Accessed 2019, Sept. 11. https://www.technologyreview.com/s/603200/voice-analysis-tech-could-diagnose-disease/

[6] Chou, Chih-Yueh et al. "Redefining the learning companion: the past, present, and future of educational agents" *Computers & Education*. vol 40. no. 3, pp. 255-269. April 2003. Accessed 2019, Sept. 16. https://perma.cc/34Z3-DLDC

[7] Manyika, James et al. "Jobs lost, jobs gained: What the future of work will mean for jobs, skills, and wages" McKinsey Global Institute. 2017, Nov. Accessed 2019, Sept. 16. https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages

[8] "The Next Era of Human-Machine Partnerships: Emerging Technologies' Impact on Society and Work in 2030." The Institute for the Future & Dell. 2017, July 12. Accessed 2019, Sept. 17. http://www.iftf.org/future-now/article-detail/realizing-2030-dell-technologies-research-explores-the-next-era-of-human-machine-partnerships/

[9] Brown, Elsa et al. "Youth and Artificial Intelligence: Where We Stand" Berkman Klein Center for Internet and Society at Harvard University. 2019, May 31. Accessed 2019, Aug. 20. https://cyber.harvard.edu/publication/2019/youth-and-artificial-intelligence/where-we-stand

[10] "The Future of Jobs Report 2018: Centre for New Economy & Society" World Economic Forum. 2018, Sept. 17. Accessed 2019, Oct. 22. https://www.weforum.org/agenda/2019/04/skills-jobs-investing-in-people-inclusive-growth/

[11] Groopman, Jessica. "Artificial Intelligence Use Cases: 258 Use Case Descriptions, Examples, and Market Sizing across Enterprise, Consumer, and Government Markets" Tractica. 2017. Accessed Sept. 2019. https://www.tractica.com/research/artificial-intelligence-use-cases/

[12] Leuth, Knud Lasse. "State of the IoT 2018: number of IoT devices now at 7B-- Market accelerating" IoT Analytics. 2018, Aug. 8. Accessed 2019, Sept. 18. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[13] Survey of 1,300 consumers to determine smart home buying criteria, by Comcast & August Home. Meola, Andrew. "People buy smart home products for this one main reason" *Business Intelligence*. 2016, Apr. 22. Accessed 2019, Sept. 14. https://www.businessinsider.com/home-security-is-number-one-driver-of-smart-home-adoption-2016-4

[14] Ibid "Connected Families: How Parents Think & Feel about Wearables, Toys, and the Internet of Things"

[15] Quito, Anne. "The wellness movement has infiltrated car design" *Quartz*. 2019, Aug. 10. Accessed 2019, Sept. 15. https://qz.com/1682045/the-wellness-movement-has-infiltrated-car-design/

[16] Ng, Alfred. "Amazon will stop selling connected toy filled with security issues" *CNET*. 2018, June 5. Accessed 2019, Sept. 6. https://www.cnet.com/news/amazon-will-stop-selling-connected-toy-cloud-pets-filled-with-security-issues/

[17] Ibid "Connected Families: How Parents Think & Feel about Wearables, Toys, and the Internet of Things"

[18] Cagiltay, Kursat et al. "Usability Study of a Smart Toy on Students with Intellectual Disabilities" *Journal of Systems Architecture*. 2018, Aug. Accessed 2019, Sept. 15. https://www.researchgate.net/publication/326859249_Usability_Study_of_a_Smart_Toy_on_Students_with_Intellectual_Disabilities

[19] Alert # I-071717 "Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children" Federal Bureau of Investigation. 2017, July 17. Accessed 2019, Sept. 10. https://www.ic3.gov/media/2017/170717.aspx

[20] **Ambient computing,** sometimes called ambient intelligence, refers to environments fully outfitted with digital networking and infrastructure to sense, adapt, respond autonomously to people and anticipate their needs. The term often characterizes the disappearance or invisibility of technology, as "intelligence" – devices or software – are embedded into physical environments like homes, offices, or hospitals.

[21] Hosein, Anesa. "Girls' video gaming behaviour and undergraduate degree selection: a secondary data analysis approach" *Computers in Human Behavior*. vol. 91, pp. 226-235. Feb. 2019. Accessed 2019, Sept. 20. https://www.sciencedirect.com/science/article/pii/S0747563218304862

[22] Mcdonald, Emma. "Newzoo's 2017 Report: Insights into the $108.9 Billion Global Games Market" *Newzoo Insights*. 2017, June 20. Accessed 2019, Sept. 16. https://newzoo.com/insights/articles/newzoo-2017-report-insights-into-the-108-9-billion-global-games-market/

[23] Cortez, Meghan. "ISTE 2017: IoT Use Case Save Money and Boost Security" *EdTech Magazine*. June 2017. Accessed 2019, Sept. 14. https://edtechmagazine.com/k12/article/2017/06/iste-2017-iot-use-can-save-money-and-boost-security-infographic

[24] Weinberger, A.H et al. "Trends in depression prevalence in the USA from 2005 to 2015: widening disparities in vulnerable groups" *Psychological Medicine,* vol. 48, no. 8, 2018 pp. 1308-1315. June 2018. Accessed 2019, Sept. 14. https://www.cambridge.org/core/journals/psychological-medicine/article/trends-in-depression-prevalence-in-the-usa-from-2005-to-2015-widening-disparities-in-vulnerable-groups/8A2904A85BB1F4436102DB78E3854E35

[25] Szymanski, Jaimy. "Prepare for the New Reality of Super Employees" Kaleido Insights. 2018, Mar. 20. Accessed 2019, Sept. 12. https://www.kaleidoinsights.com/order-reports/prepare-for-the-new-reality-of-super-employees/

[26] "7 Steps to Good Digital Parenting" Family Online Safety Institute. Accessed 2019, Oct. 22. https://www.fosi.org/good-digital-parenting/seven-steps-good-digital-parenting/

[27] Rinne, April. "4 big trends for the sharing economy in 2019" *World Economic Forum.* 2019, Jan 4. Accessed 2019, Sept. 12. https://www.weforum.org/agenda/2019/01/sharing-economy