EMBARGOED UNTIL 10 A.M. E.T. JUNE 6, 2017

Media contact: Dana Page, 202-419-4372, dpage@pewresearch.org

The Internet of Things Will Expand Connected Life Despite Concerns About Vulnerabilities, Risks and Infringements of Civil Liberties

WASHINGTON, D.C. (June 6, 2017) – The Internet of Things (IoT) will continue to spread rapidly between now and 2026 while raising a host of potential challenges, according to canvassing of more than 1,200 experts by Pew Research Center and Elon University's Imagining the Internet Center.

These experts believe further human and machine connectivity will progress despite events such as the recent WannaCry ransomware disruption and Mirai bot attack – events that highlight serious global vulnerabilities in rapidly evolving technology networks. The experts also fear that a hyperconnected world poses threats to civil liberties.

"Participants in this canvassing said a variety of forces will propel more connectivity over the next decade that manifests in things like cars, medical devices, public infrastructure and home 'smart' systems," said Lee Rainie, co-author and director of Pew Research Center's internet, technology and science research. "They argue that humans crave connection; that the IoT will bring advantages that are useful; that people's desire for convenience will usually prevail over their concerns about risk and these factors will make it difficult – if not impossible – for people to opt out of a highly connected life. At the same time, a small share of the experts predicted that significant numbers will withdraw to at least some degree from connected life due to possible risks that will arise as the IoT rolls out."

This report, part four of a five-part series on the future of the internet, is based on a nonscientific canvassing of 1,201 respondents conducted from July 1 to Aug. 12, 2016. Participants were asked the following question: *As billions more everyday objects are connected in the Internet of Things, they are sending and receiving data that enhances local, national and global systems as well as individuals' lives. But such connectedness also creates exploitable vulnerabilities. As automobiles, medical devices, smart TVs, manufacturing equipment and other tools and infrastructure are networked, is it likely that attacks, hacks or ransomware concerns in the next decade will cause significant numbers of people to decide to disconnect, or will the trend toward greater connectivity of objects and people continue unabated?* Some **15%** of these respondents said significant numbers are likely to disconnect and **85%** chose the option that most people will move more deeply into connected life.

Many participants addressed one or more of the following prompts they were asked to consider*: **1)** What is the most likely kind of physical or human damage that will occur when things are networked? **2**) How might governments and technologists respond to make things more secure and safe? **3)** Is it possible to network physical objects in such a way that they will generally remain safe for the vast majority most of the time?*

"We asked this question because powerful voices in the security community have warned about vulnerabilities posed by the spread of the Internet of Things – from heart pacemakers to highways to applications that control homes," said Janna Anderson, director of Elon University's Imagining the Internet Center and co-author of this report. "The experts we questioned in this canvassing clearly expect the IoT will continue to spread even as risks proliferate because the promise of the IoT is that lives will be healthier, safer and more convenient. At the same time, these experts argue that people are being lured or pushed into a world they don't fully understand, full of hazards that even the IoT's creators cannot fully mitigate. Most of their concerns are tied to worries over harm from bad actors and over the motivations of the corporate and government bodies that create, operate and regulate rapidly emerging complex networks. Many respondents lack faith in their capacity to perfectly plan, build, update, regulate and maintain these systems in a way that serves the public good as well as their own interests."

The analysis of overall responses uncovered the following seven themes:

People crave connection and convenience, and a tech-linked world serves both goals well

- It's only human to connect, and there are many advantages.
- As life increases in complexity, convenience is the default setting for most people
- The always-online younger generation can't imagine being anything but connected

Unplugging is nearly impossible now; by 2026 it will be even tougher

- Businesses will penalize those who disconnect; social processes reward those who connect. Fully withdrawing is extremely difficult, maybe impossible
- You can't avoid using something you can't discern. So much of the IoT operates out of sight that people will not be able to unplug completely

Risk is part of life. The Internet of Things will be accepted, despite dangers, because most people believe the worst-case scenario would never happen to them

More people will be connected *and* more will withdraw or refuse to participate

Human ingenuity and risk-mitigation strategies will make the Internet of Things safer

- Effective regulatory and technology-based remedies will emerge to reduce threats
- Governments should be doing more to regulate negligent companies, punish bad actors

Notable numbers will disconnect

- Lack of trust, safety and privacy issues and more may move those with fears to withdraw
- Corporate intransigence, shortsightedness and misguided thinking create vulnerabilities
- Oversharing and less-than-stellar performance from complex tech systems will drive dropouts

Whether or not people disconnect, the dangers are real. Security and privacy issues will be magnified by the rapid rise of the Internet of Things

- Threats are likely to turn into attacks and other acts, possibly some violent
- The rise of the IoT and security concerns amplifies endangerment of and worries over civil liberties

Following are a sample of thoughts shared by participants in the survey:

Jim Warren, longtime technology entrepreneur and activist, replied, "… from primitive Man to the present – we have almost *always* favored and pursued increased connectivity. It is the essence of society, culture, productivity, improved living and lifestyle alternatives (et al.) and *will* continue. Probably the largest deterrents to the speed and pervasiveness of its development will be largely, perhaps mostly, how much it costs its users, both financially and functionally."

Marti Hearst, a professor at the University of California, Berkeley, replied, "… it will become impossible to opt out of the oncoming connected world. People's businesses, homes, cars and even their clothing will be monitoring their every move, and potentially even their thoughts. Connected cities will track where and when people walk, initially to light their way, but eventually to monitor what they do and say. The walls of businesses will have tiny sensors embedded in them, initially to monitor for toxins and earthquakes, and eventually to monitor for intruders and company secrets being shared. People currently strap monitors on their bodies to tell them how many steps they take. Eventually, all fluids in and out of bodies will be monitored and recorded. Opting out will be out of the ordinary and hugely inconvenient, just as not carrying a mobile device and not using a fast pass on the highway are today."

Barry Chudakov, founder and principal at Sertain Research and StreamFuzion Corp., wrote, "We are witnessing the advent of what the brilliant scholar and media theorist Derrick de Kerckhove (years ago) called 'connected intelligence' – but on a scale unimaginable before the 21st century. … De Kerckhove called it a 'change of being,' which captures the breadth and depth of what is happening daily as our physical and digital objects intertwine. So not only will the trend toward greater connectivity of people and objects continue, it will continue to change boundaries and dynamics of all sorts – personal, social, moral, political. … The IoT reality represents both huge opportunity and huge vulnerability. They go hand in hand. We cannot be proactive until we educate ourselves and continue to educate others about what is required to secure IoT and what secure IoT practices entail."

David Clark, senior research scientist at MIT and Internet Hall of Fame member, replied, "Unless we have a disaster that triggers a major shift in usage, the convenience and benefits of connectivity will continue to attract users. Evidence suggests that people value convenience today over possible future negative outcomes."

Mark Lemley, a professor at Stanford Law School, commented, "There will definitely be hacks and other problems, just as there are with credit cards and financial information online today. But the advantages of connectivity are just too great for people to forgo it. We may see greater local control over when connected devices are enabled, allowing people to turn connectivity off at will."

Amy Webb, futurist and CEO at the Future Today Institute, wrote, "Technology can be like junk food. We'll consume it, even when we know it's bad for us. There is no silver bullet. The only way to effectively prevent against malware and data breaches is to stay continually vigilant. To borrow an analogy from 'Game of Thrones,' we need a 'Night's Watch' for security. Because when it comes to the Internet of Things and data breaches, 'winter is coming.' Organizations must hire enough knowledgeable staff to monitor and adjust systems, and to empower them to keep pace with hackers. IT and security staff must be willing to educate themselves, to admit when they need help and to demand that executives make decisions proactively."

Judith Donath of Harvard University's Berkman Klein Center for Internet & Society wrote, "People will move more deeply into connected life – and they also will be moved there whether they want to be or not. The connection of the physical world to information networks enables the collection of an unimaginably vast amount of data about each of us, making it possible to closely model how we think and to devise increasingly effective ways of influencing how we act and what we believe. Attaining this ability is extraordinarily valuable to anyone with something to sell or promote. … My concern with the safety of things that are part of deeply connected world is not about its security and the dangers of being hacked (though those are real, and quite serious) but with the dangers that come with their intended uses: collecting a vast amount of intimate data about each person, while weaving themselves into everyday life as a source of great convenience and pampering."

Andrew Walls, managing vice president at Gartner, replied, "The benefits of IoT to the vendors of products and services will overwhelm the objections of the few consumers who fear security issues. Pricing models will penalize those who attempt to disconnect and reward those who connect. … If IoT enhances performance against consumer variables for selection/purchase, IoT integration will expand massively."

Erik Johnston, associate professor and director of the Center for Policy Informatics at Arizona State University, observed, "Trying to disconnect in the future will be increasingly difficult. Only those who are either very privileged or unprivileged will find themselves in a situation where the majority of their lives are not connected in a meaningful way. As the default becomes … to opt in (unless there is a sea change in regulation) it will be very costly and time consuming to disconnect from each phase of life. And that is for the places where they know they are connected. It would be impossible to opt out of public surveillance, the TSA [Transportation Security Administration] and many other essentials of navigating a normal life."

Bart Knijnenburg, an assistant professor in human-centered computing at Clemson University, responded, "The immediate and concrete benefits of connectivity, however small, will outweigh the uncertain future threats, so people will choose connectivity over security. Insurance firms may capitalize on insuring against digital threats to physical devices. The only thing that may cause people to disconnect is a widespread terrorist attack against the digital infrastructure. Even if such an attack is inconsequential for people's TVs and fridges, it may change the narrative enough that people will disconnect."

Jonathan Grudin, principal researcher at Microsoft, observed, "Previous hardware generations and major software advances gave rise to fears, but people found ways to use them effectively, warranting measures to prevent serious misuse or negative consequences. Why would this be an exception?"

Robert Atkinson, president of the Information Technology and Innovation Foundation, observed, "Most adults in the U.S. drive cars even though it entails risks. Most adults will use IoT devices even though they involve risks because the benefits will vastly outweigh any potential risks. Moreover, as IoT progresses security will improve."

Jamais Cascio, distinguished fellow at the Institute for the Future, wrote, "More people will be more deeply connected, but will likely be less aware of it. Think of it as the 'electricity' effect. It's rare today to see something called out as being run on electricity (vehicles are the main exception); we just assume that a device or building or system is electricity-enabled. The default 'guitar' is electric, and acoustic guitars must be labeled. Similarly, in this decade we'll be moving quickly into a world where networked/'smart'/internet-enabled will be the default assumption, enough so that many people will stop thinking of it as new or different. You'll have people extolling the virtues of being 'unplugged' because they don't have any computers in the house and keep their mobile devices shut off, but [they'll] forget that the household appliances and carpeting and home solar power array are all deeply networked, because they don't have to think about or worry about those systems."

Patrick Tucker, technology editor at Defense One and author of "The Naked Future," wrote, "Biometric authentication and IoT military research programs such as the HACMS [High-Assurance Cyber Military Systems] program will make the Internet of Things more secure. That plus new services that spring up out of the Internet of Things ecosystem will shift the cost-benefit analysis of staying engaged and deepening engagement toward deepening."

Demian Perry, director of mobile at NPR, observed, "The problem with IoT devices is not that these devices are inherently less secure, but that the space is too new to have a mature security infrastructure. The market is likely to weed out insecure products over the long term, but it might also be helpful to have regulatory review over certain product categories, similar to the way the FDA manages food safety, or the role the National Transportation Safety Board is now playing in autonomous vehicles."

Kate Crawford, a well-known internet researcher studying how people engage with networked technologies, said, "This question assumes that disconnecting remains a socially and economically viable option. For many millions of people, it simply won't be. Quite apart from the individual use of devices and platforms, the infrastructure of everyday life will be networked. How does one 'disconnect' from your home, city, airport or health care system?"

Jason Hong, associate professor at Carnegie Mellon University, commented, "In the short term, we will see a lot more IoT-based attacks, especially ransomware attacks. However, organizations are already taking steps toward improving the situation. For example, the FTC has issued reports on IoT security and is asking the top manufacturers about their cybersecurity practices. Over time, I expect there to be more centers of excellence to help disseminate best practices for coding and managing IoT systems. Researchers will also come up with better ways for managing collections of devices as well as protecting low-end devices. It's also likely that insurance companies will help improve the state of the art by having higher premiums for

IoT companies that don't have good cybersecurity practices. Most importantly, cybersecurity is a known issue, and both IoT manufacturers and consumers are becoming savvier about the risks. So while there will be a lot of growing pains, I'm optimistic about the future of IoT."

Timothy C. Mack, managing principal at AAI Foresight, wrote, "At present, the Internet of Things is more a series of missteps than a grand design, if for no other reason than many of the large players are competitors versus cooperators and accepted protocols are still not agreed upon. As well, the 'gold rush' quality of such areas as 'smart homes' has led to shoddy design and poor construction of the physical and the digital aspects of this brave new world. As for the loss of critical safety and security through networks trying to interconnect and protect and the same time (with largely the same tools), we should expect many more disappointments in the IoT development saga."

John Markoff, senior writer at The New York Times, commented, "I see no back-to-the-land movement on the horizon."

Mike Roberts, Internet Hall of Fame member and first president and CEO of ICANN, responded, "It has been demonstrated time and again that individuals will trade privacy for convenience. ... One of the broader issues is how to deal with privacy as a social construct. Much of what we regard as privacy today is an Enlightenment idea that is associated with personal freedom and other human rights. Some regard these as 'immutable,' others as fungible in pursuit of a better life. The arguments are not going to be settled soon. Cultures of dissent will persist, and much will be made of 'off-netters,' similar to the publicity gained by today's 'off-grid' culture. Probably not a big deal in the grand scheme of things."

Stephen Downes, researcher at National Research Council Canada, said, "Disconnecting from technology isn't a viable response to attacks, hacks and the rest. People won't be looking to withdraw from modern technology, they will be looking for better and more secure modern technology."

Joel Barker, futurist and author at Infinity Limited, said, "Disconnection is the only solution to the size of the risk."

Stowe Boyd, managing director of Another Voice, wrote, "In a world in which connected driverless transportation becomes the ubiquitous and low-cost norm, few will be concerned that occasionally a hacker can take over a vehicle and crash it, especially since tens of thousands die every year in car accidents now. That example will be the instance that proves the general case. Yes, hacking will continue, and corporations and governments will fight it, but meanwhile, the overwhelming majority of human activities and finances will move online, and everything that can be connected to the web will be."

Read the full report:

On Pew Research site: http://www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications

On Imagining the Internet Center site: http://www.elon.edu/e-web/imagining/surveys/2016_survey/Internet_of_Things_Infrastructure.xhtml

For more information or to arrange an interview, please contact Dana Page at dpage@pewresearch.org or 202-419-4372