Sanja Milivojevic

34 Internet of things

Abstract: IoT systems are poised to play a critical role in today's infrastructures. These developments, though slow-paced, are followed by concerns about privacy violations and pervasive surveillance that bring new crime opportunities. IoT devices have not been designed with privacy and social implications in mind; they are developed using a technical, not sociotechnical, approach to technology development. This narrow approach is mainly responsible for vulnerabilities of systems, as well as often clumsy legal and policy attempts to 'catch up' with technology. As a result, we can expect further quests to 'patch up' glitches in technology's application and the unanticipated adverse impacts of technology on individuals and communities. Research must go beyond the usual frame of identity theft, blackmail, hacking, and profiling to explore the impact of the IoT on domestic and family abuse, intimate partner violence, and digital forensics. Community-led, interdisciplinary methodologies are helpful platforms for imagining and designing alternative futures in digital criminology, including the IoT.

Keywords: the IoT, privacy, surveillance, sociotechnical approach, interdisciplinary methodologies

The Internet of Things (IoT) has captured the attention of global media outlets, businesses, consultancy companies, researchers from STEM (science, technology, engineering, mathematics) disciplines, and to a lesser extent, social sciences in the last two decades. Whether warranted or not, some authors call the IoT systems "the next technological revolution" (Blythe et al., 2020), a ground-breaking but also disrupting innovation, particularly in the context of the so-called 'smart city' (see Smart City by Hayward). The smart city represents a novel way of managing urban environments by connecting and monitoring critical infrastructure components and services via emerging technologies (e. g., artificial intelligence—AI, machine learning, cloud computing, blockchain, data analytics, the IoT). In the smart city, the IoT plays a vital role in transport and traffic management, pollution monitoring, resource and energy management, healthcare, manufacturing, and the like, by collecting and exchanging data about the environment, optimizing services, and in doing so, enhancing the quality of life for smart city's inhabitants. At the same time, the IoT developments and deployments are followed by concerns about privacy violations and pervasive surveillance via networked objects (Maras and Wandt, 2019).

The IoT refers to the ability of everyday objects with a unique identification number and Internet Protocol addresses (which refers to the object's *unique identity*) to connect to the internet, other communication networks, and each other (*network*) via machine-to-machine communication (M2M), often without direct human intervention. Such objects generate and exchange data via sensors (*sensing and communication*, actuation capability that can capture context and provide/exchange information about

 https://doi.org/10.1515/9783111062037-035

the thing itself or its environment) and act based on data analysis. Thus, IoT technologies can be recapped as objects with unique identities, connected in a network, with the capability to sense, communicate, and perform specific actions.

The IoT's promise lies in enhancing the quality of services provided to people and improving the quality of life by harnessing the power of sensors, connectivity, data processing, and user interfaces (Saini et al., 2022). Ultimately, these systems enable the automation of tasks and save time and money for people, companies, and government agencies (Maras and Wandt, 2019). One example of the IoT is the so-called 'smart security' integrated system that often includes objects such as glass and door break detectors, motion detectors, smart doorbells, security alarms, and the like. Smart heating of homes and offices is another well-known example of the IoT systems.

Definitions and applications

There are many typologies of the IoT. By application, they can be consumer, commercial, industrial, military, and infrastructure systems. They can be autonomous or conventional (the IoT that requires human involvement and analysis) and centralized or decentralized. As mentioned above, the technology is already deployed in homes and buildings (security systems, smart TV, speakers, thermostats, lighting, home assistants, doorbells), energy networks (intelligent grid with resource optimization, monitoring real-time consumption, improving distribution within the supply chain, and sustainability), vehicles and roads (smart navigation, traffic prediction, sensors, remote software updates, predictive maintenance), and humans (wearables, smart watches, health trackers, heart implants, glasses).

While IoT has been considered the 'next big thing' in technology for quite some time (Blythe and Johnson, 2021), the technology has yet to 'cross the chasm' and become ubiquitous. Many, including the author of this entry, have been blindsided by the 'guesstimates' about the growth of this type of M2M systems. Such guesstimates were predicting that, for example, in the year 2032, each person is likely to be connected to 3,000 – 5,000 everyday things within the IoT (Milivojevic and Radulski, 2020) and that there will be more than 125 billion devices worldwide by 2030 (Riley, 2023). Just how these prophecies are being made, based on what methodology and how they seep into the academic and common knowledge are fundamental questions that, unfortunately, I must leave behind because of the word count limitation for this entry. In saying this, I would like to encourage critical contributions on this issue as a priority.

Nevertheless, we see such forecasts in almost every industry, government, or academic publication, even though, as I mentioned above, projections such as that the average UK household will have 15 internet-connected products by 2020 have been slow to materialize. The slower-than-expected pace occurred mainly because of significant privacy and security concerns caused by inadequate security provisions, such as weak default passwords, bad encryption, and lack of software updates (Blythe et al.,

2020; Blythe and Johnson, 2021). All this is not new; market innovations, products, and services are rarely designed with security or, more broadly, with social implications in mind. They are often considered as a technical innovation alone, a mathematical and engineering problem that needs to be solved via mathematical or engineering methods and equations, with very little, if any, consideration of the social aspect of such advances in the design segment of the innovation process. This linear technological approach to technology design and production is, I argue, largely responsible for vulnerabilities of systems and legal and policy attempts to 'catch up' with its deployment. Such an approach also results in never-ending quests to 'patch up' glitches in technology's application and, more worryingly, the unanticipated adverse impact technology has on individuals and communities.

The IoT crime, intelligence and surveillance: the problem, the solution, and how the solution creates a (different) problem

Scholars have highlighted the IoT's relevance for criminology since the early 2010s, stressing the potential of the technology to generate new crime opportunities, such as burglary, stalking, and sex crimes (Blythe and Johnson, 2021). As Felson and Eckert note in *Crime and Everyday Life*, technology can "leap ahead and create problems, while nonmaterial culture lags behind the technology – unable at first to address those problems" (2023: xvi). Delays in attitudes, legislation, and regulation are particularly obvious in debates around artificial intelligence (AI), especially large language and generative AI models such as OpenAI's ChatGPT (see Artificial Intelligence by Van Brakel). The IoT managed to avoid this lag due to a slower pace of technological development in this field.

The IoT's key weaknesses are linked to security and privacy, making them vulnerable to cyberattacks (Saini et al., 2022). It is often argued that the devices lack security provisions by default (Blythe et al., 2020), as they are not developed with security in mind. Given that the adoption of the technology is growing, scholars in the field of crime science suggest that the attack surface is also expanding (Johnson et al., 2022). Think, for example, about your smart doorbell (e.g., Amazon Ring) or your smart TV. Did you change the default password the device comes with? Do you even know how to enhance your security protocols? I confess I do not. Even if we do, it is often impossible to upgrade the security, as little care and attention are given to devices' crime and security implications (Johnson et al., 2022). Many IoT systems do not have a privacy policy that you sign before use, or at least they are challenging to find (Maras and Wandt, 2019). Finally, manufacturers often provide very little publicly available information about the security features of their devices (Blythe et al., 2019). Having this in mind, potential cyberattacks on networked devices can be local, for example when hackers exploit security weaknesses in the device to gain un-

authorized access to the device or the network (see Hacking by Wall). They can also be broader/global, when machines are 'hijacked' and used as botnets to carry out medium or large-scale attacks. In 2016, in one of the first global IoT attacks, hackers exploited hundreds of thousands of internet-connected devices with cameras and video recording systems. They launched Distributed Denial of Service (DDoS) attacks, shutting down Twitter and Netflix, among thousands of other businesses (Blythe and Johnson, 2021).

Another potential avenue for offenders is committing data or privacy breaches, in which people's personal data, such as personal identifiers and health information, could be exposed via the IoT. For example, a compromised microphone or video camera can allow a hacker to listen in on audio within a room or obtain the visual of the surroundings, allowing access to private conversations and other data which can be particularly important in the context of government or industry espionage (Maras and Wandt, 2019). In this example, the IoT's vulnerability to cyberattacks has been intertwined with its capacity for harmful surveillance. Yet, one must dig deep to find actual cases of IoT-based offending, other than often sensationalist news reports and the above-mentioned global-scale attacks. In this field, lab-based research—research that tests vulnerability in a simulated environment—dominates the space, pointing out potential exposures and gaps, which, it is suggested, offenders might use in the future (Blythe and Johnson, 2021; Maras and Wandt, 2019). As such, empirical research on the scale of victimization and offending, locally and globally, is warranted (see Victimization by Walklate).

In the studies of IoT-related offending academia focused traditionally on identity theft (see ID theft by Langford, Wærstad, and Svensson), blackmail, hacking into the IoT devices, and profiling—gathering data from the IoT about household occupancy to orchestrate theft (Blythe and Johnson, 2021). The role of the IoT in domestic and family abuse, intimate-partner violence, and stalking has been sporadically investigated in social sciences, including criminology (Slupska and Tanczer, 2021). Most of the existing literature on the topic has been published by STEM researchers in STEM journals, advocating, often, technological solutions for the problem, such as defensive devices like panic buttons, emergency lockets, safety bags, self-defensive jackets, intelligent bracelets, bands, and other wearables, even smart sandals and IoT robots. Google Scholar's results for 'IoT' and 'violence against women' display a range of papers from STEM disciplines with above-proposed solutions. The absence of social sciences' contribution is puzzling, given the attention paid to incidents in which the IoT systems are used as a tool of violence. Examples are discussed in a report from one of the leading technology magazines, *Wired*, on how smart tech is used for domestic abuse (July 2018), a report from technology portal *Vice* on abusers exploiting smart home devices (October 2019) and a UK parliament report on technology and domestic abuse (November 2020).

Some examples reported in the media, albeit extreme, underline the criminological relevance. In 2018, *The New York Times* reported that survivors of IoT-facilitated abuse were often subjected to dystopian activity, such as air conditioners being remotely switched off, digital front door passcodes changed every day, boiling a kettle of water to let the victims know they are being watched, and doorbells ringing without anyone

being outside (Lo, 2021). In one of the first documented court cases involving IoT abuse from 2018, an individual was convicted of stalking his estranged wife by hacking into the smart home hub and using it as a gateway to listen to her conversations and stalk her. Following this case, the Gender and Internet of Things project at University College London has concluded that there is both a lack of data on technology abuse via this technology and that tech abuse via the IoT (or tech abuse in general) is not explicitly considered in risk assessments and safety plans (Lopez-Neira et al., 2019). Authors of one of the few studies looking at the technology-facilitated abuse via the IoT correctly pointed out that such abuse is a sociotechnical issue that requires reframing in research design and approach, including technology co-creation and co-design (Slupska and Tanczer, 2021). I come to this important point at the end of this contribution.

Yet, the 'crime harvest' (see Johnson et al., 2022)—that is a wave of offending that was poised to follow the adoption of the IoT, both in terms of threats to individual consumers and access to larger critical infrastructure—is yet, if ever, to happen. Nonetheless, these narratives are carefully crafted by cybersecurity experts from big tech, who, after pointing out the 'problem'—the vulnerability of the original product or a lack of updates or security 'patches' in connected devices—offer a solution. Such solutions often consist of buying protection against the threat, preferably their own product. An example is a post on CNBC from January 2023, in which cybersecurity experts from Google-owned cybersecurity firm Mandiant pointed out IoT as the 'next big hacking prize,' only to offer the security solution by Mandiant. Other Big Tech cybersecurity experts followed suit (cf. 'The dark web's criminal minds see the Internet of Things as next big hacking prize', *CNBC Cyber Report*, 9 January 2023).

With the IoT's capacity for data aggregation, exchange, and analysis, privacy and mass surveillance issues are important caveats. As IoT devices record and transmit a staggering amount of data about users' activities, preferences, habits, purchases, and routines, some authors argue that the level of surveillance users and bystanders are subjected to is so unprecedented that it has previously been written about only in science fiction novels (Maras and Wandt, 2019). What presents a challenge to societies concerned with privacy and data protection is that IoT devices are not run by any government, but by multiple private entities.

This caveat, of course, does not mean that government agencies are not hoping to access and benefit from big data collected by the IoT systems. Law enforcement agencies worldwide have been seeking and obtaining data from smartwatches, medical devices, smart assistants (Alexa, Siri, etc.) and other IoT-based systems, successfully utilizing them in criminal investigations (Maras and Wandt, 2019). A particular use of the IoT has been identified in digital forensics, or the 'Internet of Evidence' (Milivojevic and Radulski, 2020). Recently, researchers at the University of Lausanne in Switzerland conducted experiments in which they found that IoT gadgets might be especially helpful in investigating arson. Experiments have shown that the devices, including temperature and motion sensors, smart cameras, smoke detectors, and a voice assistant, aided in establishing the precise moment/time of the fire, the room where the fire started, and enabled a reconstruction of the timeline of events (Choi, 2023). Some authors

(cf. Hany Atlam, Ahmet Alenezi, Maria Stoyanova, Aine MacDermott, Thar Baker, Shancang Li) now suggest that IoT Forensics is a new branch of digital forensics with a wide range of potential sources of evidence, such smart devices, servers, personal area networks, and cloud data.

Conclusion

IoT systems follow the familiar pattern of other technological advancements: they are considered within the 'part of the problem' and 'part of the solution' narrative. The IoT devices have not been designed with privacy and social implications in mind; they are developed using the technical, not socio-technical, approach to technology development. As this contribution demonstrates, there are many guesstimates and unknowns when it comes to this technology that requires criminologists' immediate attention.

Main takeaways

- The IoT brings new crime opportunities. Although its development has been slower than, for example, advances in AI, the IoT's key weaknesses (security and privacy) are making them vulnerable to cyberattacks and data and privacy breaches.
- The role of IoT in identity theft, blackmail, hacking and similar crimes is solidly researched (particularly by the STEM and crime science branch of criminology). This is not the case with the IoT's role in family and domestic violence.
- While offending via the IoT is not widespread, there are many 'solutions' advocated by a range of commercial actors ('solving the problem with the money' approach). Academia should be cautious about encouraging such 'solutions.'
- Surveillance via the IoT is ubiquitous and performed by a range of private actors. Government agencies are increasingly tapping into the big data generated by the IoT, hoping to gather intelligence necessary to solve criminal cases.

Future engagements

- Criminology should engage with the IoT systems, both as a potential target for offending and a tool for crime control. Some applications of the IoT in offending need more scrutiny, such as family and domestic violence. Privacy concerns and surveillance performed by the IoT need to be examined, both in terms of potential offending and crime control.
- Criminologists should not research the IoT alone, and not only in the field of crime science, as has been the case in the last twenty years. In order to grasp dynamics and challenges interdisciplinary approaches as different expertise is needed, including criminology, law, computer science, and engineering to venture past a

fragmented depiction of the much more complex picture of technological innovation. Interdisciplinarity is necessary to understand the complexities, risks, and potential remedies for the problems identified in this space.
– Empirical interdisciplinary research in digital futures is both sporadic and lacking. Lab-based research and literature reviews are helpful, but criminology needs to set new foci on understanding the nature, characteristics, and relevance of the IoT to crime, offending, victimisation, and criminal justice interventions.
– Potential future developments should not be guessed. There is no single, predetermined, or certain future. Scholarly activity is needed to move beyond mere observation by participating in future(s) co-creation and co-design through the broader process of sociotechnical innovation, with value-in-design research from a range of fields. Community-led, interdisciplinary methodologies via innovative research collaboration spaces are a platform for imagining and designing alternative futures in digital criminology.

Through this interdisciplinary and empirical research glitches, lags, and unwanted consequences of new technologies can be addressed, including the IoT. By using a sociotechnical approach in researching crime and digital technologies, new ways of creating academic knowledge and technological innovations can be forged while having a meaningful, non-digital impact in this space.

Suggested reading

Blythe, J. M., & Johnson, S. D. (2021). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*, 34(1), 97 – 125.

Johnson S. D., Blythe, J. M., Kim, E., & Sombatruang, N. (2022). Crime and the consumer Internet of Things. In M. Gill (ed.), *The Handbook of Security* (pp. 705 – 727). Cham: Springer International Publishing.

Maras, M.-H., & Wandt, A. S. (2019). Enabling mass surveillance: Data aggregation in the age of big data and the Internet of Things. *Journal of Cyber Policy*, 4(2), 160 – 177.

Milivojevic, S., & Radulski, E. M. (2020). The "future Internet" and crime: Towards a criminology of the Internet of Things. *Current Issues in Criminal Justice*, 32(2), 193 – 207.

Slupska, J., & Tanczer, L. M. (2021). Threat modelling intimate partner violence: Tech abuse as a cybersecurity challenge in the Internet of Things. In J. Bailey, A. Flynn, & N. Henry (eds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, Emerald Studies in Digital Crime, Technology and Social Harms (pp. 663 – 688). Leeds: Emerald Publishing Limited.

References

Blythe, J. M., & Johnson, S. D. (2021). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*, 34(1), 97 – 125. doi:10.1057/s41284 – 019 – 00211 – 8

Blythe, J. M., Johnson, S. D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science*, 9, 1. doi:10.1186/s40163 – 019 – 0110 – 3

Blythe, J. M., Sombatruang, N., & Johnson, S. D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? *Journal of Cybersecurity*, 5(1), tyz005. doi:10.1093/cybsec/tyz005

Choi, C. (9 May 2023). *The Internet of Things: Fire Sleuth, Fire Starter.* IEEE Spectrum. spectrum.ieee.org/iot-for-arson-forensics, accessed 19 June 2023.

Felson, M., & Eckert, M. (2023). *Crime and Everyday Life: A Brief Introduction*, 6th edition. Thousand Oaks: Sage. doi:10.4135/9781506394817

Johnson, S. D., Blythe, J. M., Kim, E., & Sombatruang, N. (2022). Crime and the consumer Internet of Things. In M. Gill (ed.), *The Handbook of Security* (pp. 705 – 727). Cham: Springer International Publishing. doi:10.1007/978-3-030-91735-7_33

Lo, M. (2021). A domestic violence dystopia: Abuse via the Internet of Things and remedies under current law note. *California Law Review*, 109(1), 277 – 316.

Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., & Tanczer, L. (2019). "Internet of Things": How abuse is getting smarter. *Safe – The Domestic Abuse Quarterly*, 63, 22 – 26. doi:10.2139/ssrn.3350615.

Maras, M.-H., & Wandt A. S. (2019). Enabling mass surveillance: Data aggregation in the age of big data and the Internet of Things. *Journal of Cyber Policy*, 4(2), 160 – 177. doi:10.1080/23738871.2019.1590437

Milivojevic, S., & Radulski, E. M. (2020). The "future Internet" and crime: Towards a criminology of the Internet of Things. *Current Issues in Criminal Justice*, 32(2), 193 – 207. doi:10.1080/10345329.2020.1733452

Riley, A. (2023). *How your smart home devices can be turned against you.* BBC Future. bbc.com/future/article/2020511-how-smart-home-devices-are-being-used-for-domestic-abuse, accessed 19 June 2023.

Saini, S., Chauhan, A., Sapra, L., & Thakur, G. (2022). Emerging trends in security, cybercrime, and digital forensics in the context of the Internet of Things. In K. Kaushik, S. Dahiya, A. Bhardwaj, & Y. Maleh (eds.), *Internet of Things and Cyber Physical Systems* (pp. 1 – 22). Boca Raton: CRC Press.

Slupska, J., & Tanczer, L. M. (2021). Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the Internet of Things. In J. Bailey, A. Flynn, & N. Henry (eds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, Emerald Studies in Digital Crime, Technology and Social Harms (pp. 663 – 688). Leeds: Emerald Publishing Limited. doi:10.1108/978-1-83982-848-520211049