Minnesota Journal of Law, Science & Technology

Volume 21 | Issue 1 Article 6

6-6-2020

Cybersecurity, Privacy, and Artificial Intelligence: An Examination of Legal Issues Surrounding the European Union General Data Protection Regulation and Autonomous Network Defense

Brandon W. Jackson

Cybersecurity, Privacy, and Artificial Intelligence: An Examination of Legal Issues Surrounding the European Union General Data Protection Regulation and Autonomous Network Defense

Brandon W. Jackson*

* The views expressed in this paper are expressly those of the author and do not reflect the views of the U.S. Government or Department of Defense. Brandon Jackson is an attorney with the Department of Defense and is a Professorial Lecture in Law at The George Washington University Law School. Special thanks to professors Paul Rosenzweig and Lala Qadir for their guidance on previous drafts. Also special thanks to my wife and family for their continued support.

INTRODUCTION

Alan Turing, in his famous 1950 paper, "Computing Machinery and Intelligence," wrote, "we may hope that machines will eventually compete with men in all purely intellectual fields."[1] This distant aspiration, expressed in the context of whether a machine can be indistinguishable from a human,[2] may soon be a modern-day reality as technological breakthroughs bring science closer to developing machines endowed with natural intellect—the concept of artificial intelligence (AI).[3] Over the past decade, advancements in big data, machine learning, algorithms, and computational power have brought research surrounding AI to new heights as the world looks to technology to address society's greatest

1. *See* Alan Turing, *Computing Machinery and Intelligence*, 59 MIND 236 433, 460 (1950), http://www.jstor.org/stable/2251299?origin=JSTOR-pdf (considering the question of whether machines can think).

2. *See* Steven Harnad, *Minds, Machines and Turing: The Indistinguishability of Indistinguishables*, 9 J. OF LOGIC, LANGUAGE, & INFO. 425 (2000), https://www.jstor.org/stable/40180236?seq=1 (describing the Turing test as a test of whether a machine can act indistinguishably from a human).

3. *See* Max Tegmark, *Benefits & Risks of Artificial Intelligence*, FUTURE OF LIFE INST., https://futureoflife.org/background/benefits-risks-of-artificial-intelligence/ (defining general and narrow concepts of artificial intelligence); *see also* NAT. SCI. & TECH. COUNCIL, EXEC. OFFICE OF THE PRESIDENT, PREPARING FOR THE FUTURE OF ARTIFICIAL INTELLIGENCE (2016) at 6, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf (offering alternative definitions of AI concepts and suggesting a problem-solution taxonomy for defining AI).

challenges.[4] However, just as our understanding of the technology progresses, so does the complexity of the underlying social and legal issues presented by computer systems that may one day be fully capable of making decisions exclusive of human intervention.[5]

AI has in recent years been thrust to the vanguard of technical development as nation states, private industries, and researchers seek to comprehend and exploit its potential.[6] While society has often embraced scientific advancements designed to augment and better the human experience, the foreseeable and speculative perils of AI create uncertainty surrounding its proliferation across society.[7] Despite this debate, it is likely that AI will be a disruptive force across industries, and cybersecurity[8] is no exception.[9] As security and privacy move to the forefront of business considerations, corporations and governments are increasingly turning towards automated processes to ensure compliance, avoid liability, and streamline operations in an era of big data.[10] The application of AI technologies to cybersecurity is in a novel state; however, fully autonomous network defense

---

4. *See* NAT. SCI. & TECH. COUNCIL, *supra* note 3 at 7 (summarizing current developments that represent the state of AI as of 2016).

5. *See* Tomaso Falchetta, *Profiling and Automated Decision Making: Is Artificial Intelligence Violating Your Right to Privacy?*, UNITED NATIONS RES. INST. FOR SOC. DEV. (Dec. 5, 2018), http://www.unrisd.org/TechAndHumanRights-Falchetta.

6. *See* NAT. SCI. & TECH. COUNCIL, *supra* note 3, at 35 (discussing challenges of AI in the context of international relations and role of AI in international conflicts, including armed conflicts).

7. *See* Tegmark, *supra* note 3 (noting that "the boundaries of AI can be uncertain and have tended to shift over time").

8. Cybersecurity is a subset of information security. For the purposes of this paper, cybersecurity refers to preventing, detecting, and responding to cyberattacks. Network security is a subset of cybersecurity that focuses on protecting data sent through or stored on networks. This paper focuses at times on network defense systems to highlight the underlying legal and policy considerations associated with information security and cybersecurity. For brevity, this paper does not fully detail various cybersecurity techniques. Only where necessary to build upon the legal analysis does this paper expound on the underlying technical considerations.

9. *See* NAT. SCI. & TECH. COUNCIL, *supra* note 3, at 35 (noting that AI already has an important role in cybersecurity).

10. *See* Travis Greene, *Explaining the 'New Normal' in Cybersecurity to the C-Suite*, FORBES (Sept. 12, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/09/12/explaining-the-new-normal-in-cybersecurity-to-the-c-suite/#3e668cf568a8 (describing the increased focus on cyber risk management by executive boards).

systems may be at society's doorstep.[11] Autonomous cybersecurity systems are expected to offer significant advantages in an era where the threat landscape is continuously expanding, and resources are increasingly strained.[12]

Autonomous cybersecurity systems are driven by data, and the European Union General Data Protection Regulation (GDPR) is an unavoidable moderator in this regard.[13] The GDPR places significant restraints on the collection and use of data in Europe.[14] Moreover, the extraterritorial nature of the regulation compounds the impact it has on global industries.[15] This paper is designed to expand discussion surrounding AI, cybersecurity, and data privacy through an exploration of the GDPR and the legal challenges this regulation poses for autonomous cybersecurity systems.[16] This paper contends that today's AI-based cybersecurity systems are likely capable of complying with the GDPR.[17] However, absent a technical solution, maintaining compliance will becoming increasingly difficult as these systems achieve greater autonomy.[18] Part I of this paper examines the practical and technical aspects of AI-based network defense systems. This includes a foundational exploration of the utility of autonomous network defense, current limitations and long-term prospects, and a brief technical overview of how AI is applied in the cyber domain. Part II examines the GDPR and analyzes the key privacy implications and legal challenges that

---

11. *See* NAT. SCI. & TECH. COUNCIL, *supra* note 3, at 36 (describing automated cybersecurity systems that have been developed, which represent a first step toward "the development of advanced, autonomous systems that can detect, evaluate, and patch software vulnerabilities before adversaries have a chance to exploit them.").

12. *Id.*

13. Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 2, 2016 O.J. L 119/1 [hereinafter GDPR].

14. *See* GDPR, art. 5; *see also* Part II Section A, *infra*.

15. *See generally* Bhaskar Chakravorti, *Why the Rest of the World Can't Free Ride on Europe's GDPR Rules*, HARV. BUS. REV. (Apr. 30, 2018), https://hbr.org/2018/04/why-the-rest-of-world-cant-free-ride-on-europes-gdpr-rules (explaining that the global nature of information technology has the effect of imposing Europe's GDPR Rules on the rest of the world).

16. *See* Part II Section A, *infra*.

17. *See* Part II Section B, *infra*.

18. *See* Part II Section C, *infra*.

this regulation poses for the development of AI-based network defense systems. Part II concludes with a discussion of legislative considerations for any future US data privacy law. Some that have been suggested include exemptions for data processing related to information security, inclusion of liability limitations, establishing permitted used of anonymized data, and defining permitted uses of repurposed data.[19]

I. AI-DRIVEN CYBERSECURITY SYSTEMS: A PRACTICAL AND TECHNICAL EXPLORATION

Enthusiasm for AI technologies has perhaps never been greater.[20] The tangible realizations and speculative promises of AI have prompted governments and industries to look towards AI as a transformational technology capable of disrupting nearly all industries.[21] An area that has received significant attention in this regard is cybersecurity.[22] The advent of cyberspace has fostered blended worlds of overlapping technologies, which are themselves vectors for disruption. For nation states, corporate entities, and private citizens alike, security in cyberspace is paramount to existing safely in an interconnected world.[23] However, adequate security in this domain remains elusive as a growing threat landscape and limited resources create more challenges than solutions.[24] This has prompted those in the cybersecurity domain to focus on AI as a remedial measure.[25] Section A explores the utility of AI in the cybersecurity domain and discusses the critical role that AI and machine learning will

---

19. *Id*.

20. *See Despite Enthusiasm for AI Adoption, Governments are Experiencing Challenges*, HELP NET SECURITY, Oct. 28, 2019, https://www.helpnetsecurity.com/2019/10/28/government-ai-adoption -challenges/ (noting that government leaders and senior information technology decision-makers in Finland, France, Germany, Norway, and U.K. are optimistic and enthusiastic about using AI in their operations).

21. *See* NAT. SCI. & TECH. COUNCIL, *supra* note 3, at 3 (describing U.S. concerns surrounding AI and noting that "AI holds the potential to be a major driver of economic growth and social progress, if industry, civil society, government, and the public work together to support development of the technology with thoughtful attention to its potential and to managing its risks.").

22. *Id*. at 36.

23. *See id*. (urging government and private entities to cooperate to apply AI to cybersecurity and ensure the security of AI systems.).

24. *Id*.

25. *Id*.

likely play in the future of network defense as security and privacy move to the forefront of business considerations. Section B examines the current state of AI applied to cybersecurity platforms, as well as the outlook for achieving greater autonomy in these systems. Lastly, Section C provides a foundational exploration of the technical aspects surrounding autonomous network defense systems. As a lead into Part II, this exploration will highlight aspects of AI-driven network defense relevant to the respective privacy and automation provisions of the GDPR.

A. THE RISE OF INTELLIGENT NETWORK DEFENSE SYSTEMS: ANTICIPATING AUTONOMOUS CYBERSECURITY

The proliferation of the internet has fostered an interconnected world where malicious actors can transcend physical and geographical barriers to cause harm. From espionage to offensive cyber operations, intellectual property theft to compromises of private information, cyberspace has precipitated a new domain to pursue traditional forms of conflict. Cyberspace has been defined by the evolution of technology, but its novelty in relation to conventional conflict is born from its applicability as a new venue for opportunity and disruption.[26] For governments, cyberspace is a domain void of geographical barriers; yet one which they are compelled to defend.[27] For corporations, security in cyberspace has become a foundational business consideration in a time when data breaches can have insurmountable consequences.

The cyber threat landscape has rapidly evolved as technology and data expand across interconnected domains of nation state activity, commerce, and public use.[28] Cyberspace is inherently blurred by rapidly evolving technologies, a broad range of actors, and the absence of an institutional hierarchy. As such, the digital world has precipitated a paradigm of new vectors for opportunity and harm. Innate to the underlying advancements in technology and increased global connectivity is

---

26. *See* NAT. SCI. & TECH. COUNCIL, *supra* note 3, at 35 (discussing the international cooperation and governance implications of AI).

27. *Id* at 3.

28. *See* COUNCIL OF ECON. ADVISORS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 4 (2018), https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf (explaining the landscape of threats posed by "malicious cyber activity").

the amplified threat to information technology systems. This hand-in-hand relationship is the fundamental quagmire of society's dependence on technology—advancements in information automation simultaneously offer ways to improve people's lives through technological means while augmenting the avenues by which we can be harmed through our use of the same technology.[29] Cybersecurity is no exception and world leaders, lawmakers, and corporate executives have taken notice.

Nation states utilize the digitally connected world to pursue traditional forms of conflict in a new medium.[30] Meanwhile, corporations are routinely faced with novel threats from state and non-state actors seeking to leverage cyberspace for criminal gain and other nefarious purposes. As many have noted, cybersecurity is now a "C-suite" issue that has the potential to disrupt business operations and undermine the integrity of an organization.[31] To appreciate the cyber threat one must look no further than recent news headlines.[32] Data breaches, theft of trade secrets, and targeted cyberattacks have in recent years plagued corporations and governments across the globe. Cyberattacks can disrupt critical infrastructure, undermine financial markets and institutions, and threaten national security.[33] The ramifications of these threats extend well beyond a disruption of business operations to include liability, regulatory penalties, loss of strategic information, and reputational damage.[34] Moreover, the externalities of

---

29. *E.g.,* NAT. SCI. & TECH. COUNCIL, *supra* note 3, at 39 ("AI can be a major driver of economic growth and social progress . . . with thoughtful attention to its potential and to managing its risks.").

30. *See* COUNCIL OF ECON. ADVISORS, *supra* note 28 at 3 (describing malicious cyber activity carried out by nation-states against other nation-states).

31. *See* Greene, *supra* note 10 (describing the increased focus on cyber risk management by corporate executive boards).

32. *See, e.g.* Alyza Sebenius & William Turton, *U.S. Officials Brace for Cyber-Attack Retaliation from Iran*, BLOOMBERG (Jan. 3, 2020), https://www.bloomberg.com/news/articles/2020-01-03/u-s-officials-brace-for-cyber-attack-retaliation-from-iran (reporting on the potential for Iranian cyber-attacks in response to U.S airstrikes on Iran).

33. Nadine Wirkuttis & Hadas Klein, *Artificial Intelligence in Cybersecurity*, 1 CYBER, INTELLIGENCE, & SECURITY 103, 104 (2017) (explaining three primary motivations underlying cyber threats: "financial, political, or military reasons").

34. *See* COUNCIL OF ECON. ADVISORS, *supra* note 28 at 33 ("The total cost of malicious cyber activity directed at U.S. entities is difficult to estimate

cyberattacks can have cascading effects on broader communities of users, business partners, industries, and governments.

The scope of harm posed by malicious cyber activity is immense and pervasive across a spectrum of institutions. Moving forward, the problem is only likely to worsen with the rise of big data, the proliferation of the Internet of Things (IoT), and the prominence of automation in nearly all aspects of society.[35] The challenge for corporate and governmental organizations is keeping up with evolving threats when resources and talent are increasingly strained. From a workforce perspective, there is simply not enough talent to go around. According to the 2017 Global Information Security Workforce Study released by the Center for Cyber Safety and Education, there will be a cybersecurity workforce shortage of 1.8 million by 2022.[36] Meanwhile, companies are increasingly subject to regulatory fines and liabilities as governments pass data privacy and breach notification laws.[37] Cybersecurity has no doubt moved to the forefront of business considerations as institutions increasingly see the need to be more vigilant in safeguarding data and responding to threats. However, acknowledging the problem is only part of finding a solution, and limited means in an expanding threat landscape are likely to challenge cybersecurity in the years to come.[38] In an effort to confront the cybersecurity challenge, institutions and security experts are

---

because . . . many data breaches go undetected, and even when they are detected, they are mostly unreported, or the final cost is unknown.").

35. *See* Remesh Ramachandran, *How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks*, ENTREPRENEUR (Sept. 14, 2019), https://www.entrepreneur.com/article/339509 (stating that the efficiency and low cost of the rise of AI can be used both for cybersecurity and for cost-effective attacks).

36. *See* (ISC)², Comment to NIST RFI – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development (2017) https://www.nist.gov/system/files/documents/2017/08/02/isc2.pdf (describing the current metrics of the cybersecurity workforce and anticipated challenges).

37. According to the National Conference of State Legislatures (NCSL), all 50 U.S. states have enacted data breach notification laws. *See Security Breach Notification Laws*, NAT'L CONF. ST. LEGIS. (Sept. 9, 2018), http://www.ncsl.org/research/telecommunications-and-information -technology/security-breach-notification-laws.aspx (providing a table of the corresponding breach notification statute for each state).

38. *See* Wirkuttis & Klein, *supra* note 33, at 115 (explaining that AI's advances still cannot fully accommodate the rapidly changing cybersecurity environment).

turning towards AI technologies and machine learning processes to alter the economics of cybersecurity.[39]

B. AN OVERVIEW OF AI, MACHINE LEARNING, AND CYBERSECURITY

In the context of cybersecurity, AI technologies can encompass a spectrum of utility ranging from automated detection to adaptive, autonomous systems capable of sharing information and acting independently of human control to protect a network or information system. While the former exists in some of today's cybersecurity systems, the latter is more akin to an ambition—feasible in the coming years only if AI technologies achieve greater autonomy.[40] To appreciate AI in the context of cybersecurity, however, it is important to first understand AI technologies as a whole. AI can be broadly viewed as a computerized system that can rationally solve complex problems or act appropriately to achieve an objective.[41] Across applications of AI, experts have more narrowly defined the scope of AI based on taxonomies that reflect the function, capabilities, or problem space of a system.[42] For example, venture capitalist Frank Chen categorizes the problem space of AI into five general groups: "logical reasoning, knowledge representation, planning and navigation, natural language processing, and perception."[43]

---

39. Raghav Bharadwaj, *Artificial Intelligence in Cybersecurity – Current Use-Cases and Capabilities*, EMERJ (July 22, 2019), https://emerj.com/ai-sector-overviews/artificial-intelligence-cybersecurity/ (surveying current and potential business uses for AI in cybersecurity).

40. *See* Bert Rankin, *AI in Cybersecurity: What Is Hype and What Is Real?,* LASTLINE (Dec. 13, 2018), https://www.lastline.com/blog/ai-technology-in-cybersecurity-what-is-hype-and-what-is-real/ (discussing the current limitations and future expectations of AI as applied to the cybersecurity field). *See also The Value of Artificial Intelligence in Cybersecurity*, PONEMON INST. (July 2018) at 10, https://www.ibm.com/downloads/cas/EX0P6YPO (finding that human intervention is still required when dealing with alerts).

41. *See* NAT. SCI. & TECH. COUNCIL, *supra* note 3 at 6-7 (offering alternative definitions of AI concepts and suggesting a problem-solution taxonomy for defining AI).

42. *See id.* at 6 (citing STUART RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH (2d ed. 2009)) (discussing AIs as "systems that think like humans . . . systems that act like humans . . . systems that think rationally . . . [and] systems that act rationally" and explaining the differences between each).

43. *Id.* at 7 (citing Frank Chen, *AI, Deep Learning, and Machine Learning: A Primer*, ANDREESSEN HOROWITZ (June 10, 2016), http://a16z.com/2016/06/10/ai-deep-learning-machines).

AI is inherently difficult to define because the application of AI technologies often flows between routine data processing by algorithmic systems and more advanced AI processes that require intelligent computer operations. It is common for a problem to be initially viewed as requiring AI to be solved when the solution ultimately requires only routine data processing.[44] Further clarification can be found by looking at how AI is used. From self-driving vehicles to diagnosing disease, AI is a burgeoning tool that, year by year, takes hold in new industries and markets. Meanwhile, on a more intimate level, our daily interaction with AI-driven products like smart speakers and facial recognition tools are inconspicuously and rapidly altering the human relationship with technology. These forms of AI, commonly referred to as *Narrow AI*,[45] have already proliferated across society and enhanced how we use technology for common tasks. Meanwhile, the future of AI technologies lies in *General AI*—systems capable of demonstrating intelligent behavior to process cognitive tasks.[46] While Narrow AI enables machines to complete a defined task in a manner beyond that of which a human can do, General AI has the potential to surpass human performance in nearly every cognitive process.[47] In the context of cybersecurity, a General AI system would be that which employs predictive and adaptive information security or network defense techniques to communicate between systems and act independent of human control.

At its core, AI can be viewed as the pursuit of applications that can systemically produce intelligent behavior.[48] However,

---

44. *Id.* ("In some cases, opinion may shift, meaning that a problem is considered as requiring AI before it has been solved, but once a solution is well known it is considered routing data processing.").

45. Narrow AI is "narrow" in that a new system must be developed for each new application. *See id.* at 7 n.12 ("Narrow AI is not a single technical approach, but rather a set of discrete problems whose solutions rely on a toolkit of AI methods along with some problem-specific algorithms.").

46. *Id.* at 7 ("*General AI* . . . refers to a notional future AI system that exhibits apparently intelligent behavior at least as advanced as a person across the full range of cognitive tasks.") (emphasis in original).

47. *See* Tegmark, *supra* note 3 ("While narrow AI may outperform humans at whatever its specific task is, like playing chess or solving equations, AGI would outperform humans at nearly every cognitive task.").

48. *See* NAT. SCI. & TECH. COUNCIL, *supra* note 3, at 7 ("Although the boundaries of AI can be uncertain and have tended to shift over time, what is important is that a core objective of AI research and applications over the years has been to automate or replicate intelligent behavior.").

the breadth and application of AI is vast, and there are no universal definitions for AI and the subsets of AI-related technologies and processes.[49] It is important to recognize how ambiguously defined AI impacts the development and proliferation of the technology. This is immediately apparent when looking at the short-term limitations and long-term prospects of AI in cybersecurity. Vendors are increasingly advertising AI-driven cybersecurity solutions capable of detecting threats and responding to intrusions even before they develop into a full breach.[50] However, many experts believe that this advertising is misleading.[51] While these systems do employ AI-based techniques to detect malware and recognize anomalous patterns, the systems still fall under the category of Narrow AI and likely fall short of touted expectations.[52] This concept becomes more apparent when looking at the intrusion detection systems commonly used today.

Intrusion detection systems monitor a network or system looking for malicious activity that violates a defined rule. They are typically either network or host-based;[53] however, they can also be characterized by how they detect malicious activity. Such methods generally fall into two categories: signature-based detection that identifies defined sequences within strings of data,[54] or anomaly-based detection that looks for patterns outside of defined baselines.[55] Anomaly-based detection often relies on machine learning, a subset of AI that uses algorithms to statistically evaluate large amounts of data to repeatedly refine its decision-making process and outcomes.[56] While these systems are more capable of "learning" and recognizing patterns

---

49. *See id.* at 6–7.

50. *See generally*, Lily H. Newman, *AI Can Help Cybersecurity – If It Can Fight Through the Hype*, WIRED (Apr. 29, 2018), https://www.wired.com/story/ai-machine-learning-cybersecurity/ (criticizing machine learning cybersecurity solutions that are advertised as "AI Driven").

51. *Id*.

52. *Id*.

53. *See, e.g.*, Christopher Day, *Intrusion and Prevention Detection Systems, in* COMPUTER AND INFORMATION SECURITY HANDBOOK 63–66 (2009) (discussing the advantages and disadvantages of host-based and network-based intrusion detection systems).

54. *Id.*

55. *See* Wirkuttis & Klein, *supra* note 33, at 107 (describing the two main principles for intrusion detection prevention systems (IDPS)).

56. *See generally* Newman, *supra* note 50.

to keep up with evolving cyberattacks, they are still primarily detection systems that require human programming and control.[57] In a sense, the application of machine learning techniques to network defense systems can be viewed as an extension of rules-based systems. This can be thought of as automated processes designed to make cybersecurity threat detection and mitigation efforts more efficient and effective while still requiring a degree of human control. Although they utilize advanced machine learning techniques, they are a far cry from General AI.

Deep learning—using neural network models to mimic human thinking—is a subset of machine learning. Nidhi Chappel, the Director of Machine Learning at Intel, described this technique as "machines learning on their own without explicit programming."[58] She analogized this process to how a child learns societal norms by observing the world without having to be explicitly told the rules.[59] For cybersecurity, deep learning is another step towards truly autonomous network defense and has already demonstrated some utility.[60] For example, deep learning approaches have enhanced malware identification and have thereby reduced false positives and negatives.[61] It is important to note, however, that even systems trained using deep learning are only preventive to an extent.[62] They are still primarily driven by a detect-and-respond model that is less conducive to an evolving threat landscape.[63] Moving forward, experts believe that AI will have a significant impact

---

57. *See id.*

58. Deb M. Landau, *Artificial Intelligence and Machine Learning: How Computers Learn*, IQ (Aug. 17, 2016) (quoting Nidhi Chappel).

59. *Id.*

60. *See* Raffael Marty, *AI in Cybersecurity: Where We Stand & Where We Need to Go*, DARKREADING (Jan. 11, 2018), https://www.darkreading.com/threat-intelligence/ai-in-cybersecurity-where-we-stand-and-where-we-need-to-go/a/d-id/1330787 ("Today's approaches in malware identification have greatly benefited from deep learning, which has helped drop false positive rates to very low numbers while reducing the false negative rates at the same time.").

61. *Id.*

62. *See id.* (explaining that unsupervised machine learning is still not ideal for locating anomalies, and, while supervised machine learning has been more effective for malware, it lacks good data sets for most other areas, preventing the training of algorithms).

63. *Id.*

on cybersecurity.[64] These technologies are expected to offer a more preventive solution that can classify cyber threats in real-time and detect never-before-seen activity, such as zero-day exploits.[65] Experts anticipate these systems will eventually be capable of taking action with little human input or even without intervention from a network operator.[66]

The current state of autonomous cybersecurity systems is blurred by a fog of promises from cybersecurity vendors.[67] Many companies advertise systems that use AI technologies capable of preventing attacks.[68] However, experts have suggested that these guarantees are more marketing than technique.[69] Many of the products still employ learning approaches that require human operators to tag data used to train algorithms. While security companies are deploying systems that employ machine learning approaches, fully autonomous network defense systems are still more of a dream than a reality.[70] Embellished promises and a lack of understanding of how these systems can easily cloud the state of AI in the cybersecurity industry. Notwithstanding, the likelihood of greater autonomy in cybersecurity systems seems encouraging. Researchers continue to push the bounds of AI to reduce the blind spots associated

---

64. *See generally Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy: Hearing Before the Subcomm. on Info. Tech. of the H. Oversight Comm.*, 115th Cong. (2018) (statement of Ben Buchanan, Postdoctoral Fellow, Belfer Center Cybersecurity Project, Harvard University), Prepared Testimony and Statement for the Record of Ben Buchanan, Postdoctoral Fellow, Belfer Center Cybersecurity Project, Harvard University, House Oversight Committee, Subcommittee on IT (Apr. 6, 2018).

65. *See generally* Laurent Gil, *The Debate Is Over: Artificial Intelligence Is the Future of Cybersecurity*, THE CYBERSECURITY SOURCE (Mar. 22, 2018), https://www.scmagazine.com/home/opinions/blogs/executive-insight/the-debate-is-over-artificial-intelligence-is-the-future-for-cybersecurity/ (explaining why AI is the only viable option for future cybersecurity systems).

66. *Id.*

67. *See* Newman, *supra* note 50 ("Machine learning's biggest strength in security is training to understand what is 'baseline' or 'normal' for a system, and then flagging anything unusual for human review.").

68. *Id.*

69. *See generally id.*

70. *See* Scott Finnie, *AI in Cybersecurity: What Works and What Doesn't*, CSO ONLINE (Aug. 15, 2018), https://www.csoonline.com/article/3295596/security/ai-in-cybersecurity-what-works-and-what-doesnt.html ("Much of what we hear about artificial intelligence and machine learning in security products is steeped in marketing, making it hard to know what these tools actually do.").

with traditional network defense systems. As AI technologies and deep learning techniques proliferate, it is likely that AI-based systems will require less and less human interaction.

In the cybersecurity domain, the capacity to detect and respond to intrusions is dependent on the ability to collect, process and analyze data. AI-based cybersecurity systems enhance this process through a combination of automation and advanced algorithms. The success of these systems is dependent on the availability of large quantities of quality data.[71] Traditionally, vast amounts of data have made it difficult for network defenders to distinguish relevant data and make connections across data sets. In contrast, machine learning thrives off data and offers significant advantages in this regard.[72] More data allows AI-based cybersecurity systems to establish a baseline of normal network activity or system behavior. Using an anomaly detection approach, these systems can then better detect changes or abnormalities in the network.[73] Alternatively, these systems can use large amounts of data to employ a misuse detection approach that identifies malicious activity by defining patterns of abnormal behavior in the network or system.[74]

In its current state, AI-based cybersecurity systems still require some level of human intervention. While today's systems make the threat detection process more efficient and empower security analysts to make connections in a dynamic threat environment, human decision-making is a requirement nonetheless.[75] Notwithstanding, advancements in deep learning and artificial neural networks show promise in achieving greater autonomy in the cybersecurity domain. Beyond improvements in the underlying algorithms, progress in the field of AI-based cybersecurity will be dependent on the availability of data sets. As such, it is likely that data privacy will weigh heavily in the

---

71. *See* Marty, *supra* note 60 (arguing that machine learning requires large amounts of training data to be practically employed as a cybersecurity solution).

72. *See id.*

73. *See* Wirkuttis & Klein, *supra* note 33, at 107 (describing the misuse detection approach and the anomaly detection approach associated with intrusion detection prevention systems).

74. *Id.*

75. *Id.* at 114 (noting that expert systems have only progressed to the point of assisting decision makers and do not substitute for them).

development, proliferation, and overall utility of AI-based cybersecurity systems.

C. A TECHNICAL PRIMER ON MACHINE LEARNING AND CYBERSECURITY: WHAT IT LOOKS LIKE, WHERE IT IS GOING, AND ITS RELATION TO DATA PRIVACY

Cybersecurity is premised on identifying malicious activity within a host, system, or network.[76] This inherently requires network defenders to differentiate between permissible activity and malicious behavior, a nuanced task that can prove challenging when malicious intent is rarely apparent.[77] Often the distinguishing element is simply context.[78] Whether it is downloading a malicious file or copying permitted software, network traffic often looks the same.[79] Put another way, the only difference between permitted network activity and malicious behavior is often the context of data flow. Machine learning seeks to address this challenge by leveraging large amounts of data to establish a baseline (i.e. what is "normal"), distinguish anomalies, and attribute such deviations to malicious network behavior.[80] There are two primary approaches to machine learning: supervised and unsupervised learning.[81] Supervised machine learning relies on large sets of labeled data to train algorithms as to what is "good" or "bad."[82] This approach has demonstrated significant utility for combating malware and spam because of the availability of large sets of labeled samples.[83] However, in scenarios where good data sets are limited, such as detecting network attacks, supervised machine learning would prove less useful because there is insufficient

---

76. *See generally* Marty, *supra* note 60.

77. *See id.* (stating that the primary task of machine learning is to "find anomalies" and acknowledging the difficulties of this form of threat detection with limited training data).

78. *Id.* (explaining that context alleviates challenges in identifying anomalies with machine learning).

79. *See id.* ("For example, can you define what is normal behavior for your laptop day in, day out? Don't forget to think of that new application you downloaded recently. How do you differentiate that from a download triggered by an attacker?").

80. *See id.*

81. *Id.*

82. *Id.*

83. *Id.* ("The two poster use cases [for success in machine learning] are malware identification and spam detection.").

data to establish a baseline for anomaly detection.[84] Unsupervised learning is another approach used to train algorithms. This entails various techniques, such as dimensionality reduction, clustering, and association rule learning, designed to make data easier to analyze and understand.[85] While these techniques are beyond the scope of this paper, they can best be thought of as ways to find or describe hidden structures in data.[86]

Two principal considerations in the context of machine learning, cybersecurity, and data privacy are the types of data relevant to AI-based network defense systems and how that data is used. The first consideration can be broad and is often heavily dependent on the nature of the cyber threat in question. Examples of relevant data points are IP addresses, domain names, host names, port numbers, file names, registry data, commands, usernames, email addresses, and hashes. All of this information can be broadly classified as threat indicators. The second consideration, how data is used, also significantly depends on the nature of the cyber threat. For the purposes of this paper, how data is used is best viewed in the context of cyber threat intelligence and how it is leveraged to protect networks and systems. Cyber threat intelligence is threat data that has been collected, evaluated, and analyzed by experts using structured tradecraft.[87] It is fueled by an intelligence cycle that leverages advanced toolsets and human expertise to identify and attribute cyber threats.

A significant piece of this process is information sharing that leverages the collective knowledge, experience, and capabilities of whole communities to better understand cyber threats.[88] There are sector-specific Information Sharing and

---

84. *Id.* (describing limitations to supervised machine learning).

85. *Id.* (discussing different applications for unsupervised machine learning).

86. *See id.*

87. *See* Intel & Analysis Working Group, *What Is Cyber Threat Intelligence?*, CENTER FOR INTERNET SECURITY (n.d.), https://www.cisecurity.org/blog/what-is-cyber-threat-intelligence/. ("Cyber threat intelligence is what cyber threat information becomes once it has been collected, evaluated in the context of its source and reliability, and analyzed through rigorous and structured tradecraft techniques by those with substantive expertise and access to all-source information.").

88. *See* NIST, SPECIAL PUBLICATION 800-150, GUIDE TO CYBER THREAT INFORMATION SHARING at iii (2016),

Analysis Centers (ISACs) and private entities within the United States and internationally that implement similar sharing programs.[89] For example, the Financial Services Information Sharing and Analysis Center is the central resource for cyber and physical threat intelligence analysis and sharing amongst the global financial industry.[90] In addition to specific indicators, ISACs often share tactics, techniques, and procedures, security alerts, threat intelligence reports, and tool configurations.[91] Such sharing no doubt enhances cybersecurity across the globe; however, it can be a double-edged sword when data privacy is taken into account.[92]

A key challenge for sharing threat information is protecting against unauthorized disclosure of personal data.[93] This has prompted ISACs and similar entities to employ detailed sharing policies and procedures to safeguard privacy in the digital world.[94] Today, the sharing process is highlighted by extensive human control.[95] Indicators are vetted and threat information is stripped of personal data before being disseminated to larger groups.[96] However, this process will likely change as AI-driven systems increasingly replace human judgment to make determinations and share information. This paradigm may be especially challenging when considered in the context of the black box problem—the idea that an advanced system can produce a result without any evidence as to how it arrived at its

---

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf ("By exchanging cyber threat information within a sharing community, organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain more complete understanding of the threats the organization may face.").

89. *See, e.g.*, FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER (FSISAC), https://www.fsisac.com/ (last visited Feb. 8, 2020).

90. *See generally id*.

91. *See* NIST 800-150, *supra* note 88, at ii ("Cyber threat information includes indicators of compromise; tactics, techniques, and procedures used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents.").

92. *See id*. at 4–5 (highlighting concerns relating to safeguarding personal information and trade secrets when exchanging information on cyber threats).

93. *See id.* at 4 (listing the "[d]isclosure of sensitive information, such as . . . personally identifiable information" as one of the challenges of information sharing).

94. *See id.* (providing guidelines for establishing and participating in sharing relationships).

95. *See, e.g.*, *id*. (outlining regulations for information sharing).

96. *See id*. at 11.

decision.[97] The effectiveness of tomorrow's cybersecurity systems could very well depend on the availability and sharing of information that may directly or indirectly involve personal data. Moving forward, this could pose significant challenges for engineers and lawmakers as society seeks to balance cybersecurity needs and data privacy concerns.

II. THE GENERAL DATA PROTECTION REGULATION: AUTONOMOUS CYBERSECURITY AND DATA PRIVACY

The proliferation of technologies across nearly all domains is altering the foundation of civilization. Never before in the history of humankind have societies been more connected, as emerging technologies foster unparalleled ways to for us to communicate our identity to the world—intentionally or unintentionally. In the wake of society's technological growth, we are now faced with the challenges of our technological supremacy, and data privacy is taking center stage.[98] Society continues to immerse itself in computerized machinery prompting each individual to leave a digital footprint[99] that is often more revealing of a person's being than any other form of communication. While there are benefits and conveniences to projecting one's digital self to the world, it can also be fraught with uncertainty, lack of control, and abusive practices that threaten the very utility of the underlying technologies.[100] This has prompted lawmakers to direct significant attention to data privacy, and Europe has taken the lead.

---

97. *See* Brandon Buckner, *How Can We Trust Decisions Made by AI?*, Leidos: Insights (Apr. 15, 2019), https://www.leidos.com/insights/how-can-we-trust-decisions-made-ai (stating that decisions made by AI and machine learning techniques are often made in a "black box" and that tracing a point back to its origin is not yet a part of AI and machine learning).

98. *See, e.g.*, Paul Smits, *Legal Specialist: New Technology Forces Update of Data Privacy Laws*, INNOVATION ORIGINS (Feb. 9, 2020), https://innovationorigins.com/legal-specialist-new-technology-forces-update-of-data-privacy-laws/ (interviewing legal privacy expert, Jeroen Terstegge, who believes the emergence of new technologies prompts an update in the General Data Protection Regulation).

99. *See Digital Footprint*, TECHTERMS, https://techterms.com/definition/digital_footprint (last visited Feb. 9, 2020) (defining "digital footprint" as "a trail of data you create while using the Internet").

100. *See, e.g.*, *id.* ("[O]nce digital data has been shared online, there is no guarantee you will ever be able to remove it from the Internet.").

Part II of this paper explores the GDPR[101] as it relates to AI-based network defense systems. It offers two key findings: first, compliance under the GDPR may be challenging but still possible for today's AI-based cybersecurity systems, and second, absent a technological solution, it will become increasingly difficult for these systems to maintain GDPR compliance as the underlying AI technologies achieve greater autonomy. Section A examines how the GDPR applies to AI and network defense and discusses the compliance challenges posed by this regulation. Section B examines the larger challenges of GDPR compliance associated with training algorithms and information sharing. Section C looks at the future of AI-based network defense and how these challenges will be compounded as AI-based network defense systems move towards greater autonomy and may be less capable of protecting personal data. Lastly, Section D highlights the growing consensus within the US for a national data privacy law and identifies key features that may minimize data privacy issues in cybersecurity and promote the overall development of autonomous network defense systems.

A. THE GENERAL DATA PROTECTION REGULATION APPLIED TO AI-BASED NETWORK DEFENSE: LEGAL QUESTIONS AND CHALLENGES

In 2016, the European Union (EU) Parliament passed the most significant data privacy regulation in decades. The GDPR, which took effect on May 25, 2018, provides EU citizens with extensive data privacy and protection rights that are designed to protect[102] European citizens and harmonize data privacy laws across Europe.[103] However, the regulation extends beyond the EU to reach European citizens worldwide and businesses outside of Europe that handle the personal data of EU citizens.[104] On its face, the GDPR does not seem to be a regulation that would govern cybersecurity and network defense. Rather, data privacy suggests protecting personal data

---

101. *See generally*, GDPR.

102. *See* GDPR, pmbl. (1) (declaring protection of personal data a fundamental right).

103. *See* David Bender, *GDPR Harmonization: Reality or Myth?,* IAPP (June 7, 2018), https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/.

104. *See generally* Chakravorti, *supra* note 15 (explaining that the global nature of information technology has the effect of imposing Europe's GDPR Rules on the rest of the world).

used for things like social media or financial transactions. But if one looks deeper, the connection between personal data and cybersecurity is more apparent. In the context of AI-based network defense, the association with data processing is primarily derived from two separate components of the automated threat intelligence life cycle: personal data used to train a network defense algorithm and personal data used in the cyber threat intelligence sharing process.[105]

1. The GDPR: Scope

The GDPR applies to the "processing of personal data" by a "controller" or "processor" regardless of whether the processing takes place in the EU.[106] The GDPR also applies to the processing of the personal data, of data subjects who are in the EU, by a "controller" or "processor" outside of the EU, when the processing relates to the offering of goods or services to EU citizens or the monitoring of EU citizens' behavior that takes place in the EU.[107] To fully unpack the scope of the GDPR and understand the extent of this regulation, one must look at how the regulation defines "personal data" and "processing," as these terms collectively expand the material scope of the GDPR:[108]

> **Personal Data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;[109]
>
> **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making

105. *See supra* Section I part C (discussing the ways that A.I. uses data in network defense).

106. GDPR, art. 3(1).

107. *Id.* at art. 3(2)(a)–(b).

108. Matthew Humerick, *Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence*, 34 SANTA CLARA HIGH TECH. L.J. 393, 402 (2018) (suggesting that definitions of "personal data" and "processing" serve to expand the material scope of the GDPR).

109. GDPR, art. 4(1).

> available, alignment or combination, restriction, erasure or destruction . . . .[110]

AI-based network defense systems primarily fall within the scope of the GDPR through either the use of personal data to train algorithms or when personal data is used in the cyber threat intelligence sharing process. Both scenarios raise questions of whether an entity can be considered a "controller" or "processor," and whether certain indicators are considered personal data. As noted above, a "controller" is an entity that determines the purposes and means of the processing of data,[111] and a "processor" is an entity that processes personal data on behalf of a controller.[112] In network defense and the cyber threat information life cycle, this encompasses any entity that collects and stores data, shares information, or uses data for machine learning. This could include developers, security vendors, ISACs, or entities that have employed a particular AI-based network defense system because these entities are all involved in operations performed on personal data. In many cases an entity could be considered both a "controller" and a "processor" depending on the operational data role.[113]

The next question is whether the relevant data is even considered personal data. As discussed above, network defense is fueled by known indicators, and these indicators often include personal data. Some indicators, such as email addresses, usernames, or payment transactions, are more obviously associated with personal data.[114] These types of indicators can be used, directly or indirectly, to identify a natural person. In other circumstances, whether an indicator constitutes personal data is less apparent and often depends on how it is used. One of the most common cyber threat indicators is an internet protocol (IP) address, and European courts have found that IP addresses are protected personal data because they allow users

---

110. *Id.* at art. 4(2).

111. *Id.* at art. 4(7).

112. *Id.* at art. 4(8).

113. For example, a cybersecurity vendor could be considered a controller when it is processing data it collects and aggregates from various sources but also be considered a processor when it is only processing data on behalf of a particular client.

114. *See, e.g.*, *What Is Personal Data?*, EU GDPR COMPLIANT (last visited Feb. 9, 2020) (listing full names, email addresses, and credit card numbers as examples of classical personal data), https://eugdprcompliant.com/personal-data/.

to be precisely identified.[115] Even dynamic IP addresses, those which are temporarily assigned to a computing device, can be considered personal data when a controller has legal means to identify a data subject in conjunction with additional data that may be available.[116] Under this principle, indicators could individually fall out of the scope of personal data. However, when means exist to augment data with other information to identify a data subject, the initial indicator could then be viewed as personal data. For example, a user's search queries may only become personal data when a processor has access to IP records associated with the data subject that could then identify the natural person.[117]

2. The GDPR: Key Features and Principles

The GDPR consists of ninety-nine articles that collectively aim to regulate data processing and provide a uniform approach to data privacy.[118] At its core, however, are specific principles set forth in Article 5.[119] These key principles relating to the processing of personal data include lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.[120] For those developing or using AI systems that utilize data from EU citizens, the GDPR can be an unavoidable force. In the age of big data and automation, the extraterritorial nature of the regulation can easily bring non-EU corporations within EU jurisdiction.[121] Moreover, subjected entities can face administrative fines up to 20,000,000 EUR or up to four percent of the total worldwide annual turnover of the preceding financial

115. *See* Case C-70/10, *Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Èditeurs*, 2011 E.C.R. I-11959, para. 26. (describing IP addresses as personal data).

116. *See* Case C-582/14, *Breyer v. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, para. 49 (holding that dynamic IP addresses are personal data within the meaning of former GDPR Article 2(a) under such circumstances).

117. *See, e.g., id*. (holding that a dynamic IP address can constitute personal data if an online services provider possesses the ability to identify the subject using the IP address in conjunction with other information).

118. *See generally* GDPR.

119. *See* GDPR, art. 5(1)(a)–(f).

120. *Id.*

121. *See* GDPR, art. 3 (establishing the extraterritorial scope of the GDPR).

year.[122] The collective utility of the GDPR is up for debate. On one hand, it can be argued that the law is about protecting citizens by setting forth requirements and standards for data processing and information sharing.[123] On the other, the GDPR can be viewed as a regulation with geopolitical intentions meant to strengthen Europe's political power in the digital age.[124] Regardless of its purpose, the GDPR cannot be ignored, and there are several key provisions relevant to AI, cybersecurity, and information sharing. These include provisions related to the right to consent, the right to be forgotten, the right to an explanation, and the right to data portability.

A key feature of the GDPR is consent. Article 4(1) requires that consent be "freely given, specific, informed, and unambiguous."[125] Furthermore, the GDPR adopts an opt-in approach to consent that requires controllers to be able to demonstrate that the data subject has consented,[126] and such consent can be withdrawn at any time.[127] Data subjects can also restrict processing of personal data under certain circumstances.[128] These include instances where a data subject contests the accuracy of personal data, the data subject believes the processing is unlawful but data erasure is not a suitable remedy, the controller no longer needs the personal data but must maintain it for legal claims of the data subject, or when the data subject has objected to processing based on legitimate grounds.[129] For machine learning, these consent requirements

---

122. GDPR, art. 83.

123. *See* GDPR, art. 1(1) ("This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.").

124. *See* Roslyn Layton & Julian Mclendon, *The GDPR: What It Really Does and How the U.S. Can Chart a Better Course*, 19 FEDERALIST SOC'Y REV. 234, 236 (2018) (suggesting that the primary goals of the GDPR are geopolitical, including "(1) solidifying legitimacy for Brussels during a period of skepticism among voters, and (2) strengthening European political power against the real or perceived threat of American digital prowess").

125. GDPR, art. 4(11).

126. *See* GDPR, art. 7(1) ("Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.").

127. *See* GDPR, art. 7(3) ("The data subject shall have the right to withdraw his or her consent at any time.").

128. *See* GDPR, art. 18 ("The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies . . . .").

129. *See id*.

can prove challenging because it can limit the amount of data initially available and can impact the training model when data is subsequently removed.[130] Prior learning may be valid, but derivative learning processes could risk GDPR noncompliance.[131] Moving forward, these technical realities are likely to challenge engineers and legal experts seeking to promote compliant processes.

Another key feature of the GDPR relates to erasing data—the "right to be forgotten."[132] Under Article 17, controllers are obligated to erase all personal data under certain conditions.[133] Instances that warrant erasure of data include when the data is no longer necessary in relation to the purpose for which it was collected and when consent has been withdrawn.[134] Similar to the consent issue, this can create significant challenges for AI. The utility of algorithms trained on machine learning processes stems from the training data.[135] If data is subsequently removed, this can disrupt the algorithm's future behavior and create inaccurate or unreliable results.[136] Although companies could train algorithms on updated datasets, this may create additional risk and liabilities given the volatility and uncertainty if significant portions of training data can be so easily removed.[137] In the context of cybersecurity, this could prove disastrous. For example, if a large dataset of IP addresses was removed from a training model, then the baseline for the network defense system may be altered and no longer be reliable in detecting anomalies.[138] Also, in some instances the technical realities of isolating and deleting data may make compliance overly burdensome. Some commentators have even suggested that the

---

130. *See* Humerick, *supra* note 108, at 406 ("Both the need for consent and the right [to] withdraw consent threaten the development of AI because it could limit the amount of data available to learn from.").

131. *See id*. (suggesting that when consent to use data is withdrawn "further processing of and learning from these specific data points would constitute a violation of the GDPR").

132. GDPR, art. 17.

133. *Id.*

134. *Id.*

135. *See* Humerick, *supra* note 108, at 408 (noting this impact that data erasure may have on the accuracy and reliability of an AI system).

136. *See id.*

137. See *id.*

138. *See supra* Part I Section B (discussing how anomaly detection requires processing of sufficient data sets).

technical requirements of data deletion could make compliance nearly impossible.[139] Companies that are unable to isolate indicators that fall under the GDPR would risk noncompliance by continuing to operate their systems.

Another prominent component of the GDPR as it relates to AI is the right to an explanation. Article 22 governs automated individual decision-making,[140] which is often a key feature of AI systems.[141] This article provides data subjects with the right to not be subject to decisions based solely on automated processing, including profiling, that produce a legal effect concerning the data subject.[142] While there are stated exceptions, such as public interest or performance of a contract,[143] uncertainty as to what meets an exception should warrant reservations for those looking to maintain compliance.[144] Furthermore, the automated processing provisions require that any subject decisions be explainable.[145] This can prove challenging, especially in the context of unsupervised learning, when engineers cannot trace the learning process or understand why the system made its

---

139. *See generally* Edward F. Villaronga, Peter Kieseberg, & Tiffany Li, *Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten*, 34 COMPUT. L. & SEC. REV., 304 (2018) (discussing the difficulties that arise in trying to erase data).

140. *See* GDPR, art. 22 (providing provisions relating to "[a]utomated individual decision-making, including profiling").

141. *See* Falchetta, *supra* note 5 (explaining that AI applications are used to "automatically sort, score, categorize, assess and rank people").

142. *See* GDPR, art. 22(1) ("The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.").

143. *See id.* at art. 22(2), 46 (providing exceptions for when data subjects may be able to be subject to a decision based solely on automatic processing that produce a legal effect).

144. *See* Eduardo Ustaran & Victoria Hordern, *Automated Decision-Making Under the GDPR—A Right for Individuals or a Prohibition for Controllers*, HOGAN LOVELLS: CHRONICLE OF DATA PROTECTION (Oct. 20, 2017), https://www.hldataprotection.com/2017/10/articles/international-eu-privacy/automated-decision-making-under-the-gdpr-a-right-for-individuals-or-a-prohibition-for-controllers/ (discussing the "considerable uncertainty" with respect to Article 22 of the GDPR).

145. *See* GDPR, art. 22(3) ("[T]he data controller shall implement suitable measures to safeguard the data subject's rights . . . at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.").

decision.[146] As noted earlier, this is the black box problem.[147] In the context of cybersecurity and information sharing, this can be a significant challenge when threat information is derived from protected information and automatically shared with another system or entity.

On its face, GDPR compliance for automated processing is more akin to automated decisions that are closely aligned with the rights of a natural person, such as access to health care or criminal sentencing. However, automated decision processing exists in the cyber world as well and can have significant ramifications for users. This is especially true when participation in society increasingly requires access to information and the interconnected global domain. Imagine an individual whose login credentials are revoked after an automated system made a determination that revocation was necessary to protect the network.[148] As AI moves towards greater autonomy and requires less human intervention, this is a scenario that may become more likely.[149] In this instance, it is possible that network administrators would not be able to explain why the system revoked access.[150] Although loss of access may not always be significant, the overarching issue is likely to warrant concern for companies seeking to promote compliant technology.[151]

A final prominent feature of the GDPR that is relevant to AI is the right to data portability. Under Article 20, a data subject has a right to receive personal data concerning him or her and to transfer personal data from one controller to another.[152] This creates some of the same issues posed by to the rights to consent

---

146. *See* Buckner, *supra* note 97.

147. *Supra* Part I, Section C.

148. *See, e.g.*, Lee Painter, *Could AI Improve Identity Management and Security*, CATAPULT DIGITAL (May 25, 2017), https://www.digicatapult.org.uk/news-and-views/blog/could-ai-improve-identity-management-and-security/ (describing the use of AI to determine if a user should be able to access a network).

149. *See generally* Buckner, *supra* note 97.

150. *Id*.

151. *See* GDPR, art. 22(2), at 46 (indicating that the automated decisions must be explicable).

152. GDPR, art. 20(1), at 45 ("[T]he data subject shall have the right to receive the personal data concerning him or her . . . in a structured, commonly used and machine-readable format . . . .").

and erasure,[153] but it also creates practical challenges for the cybersecurity industry. The utility of AI-based network defense systems is derived from the underlying data sets and algorithms.[154] In most cases, users of these systems will have consented to use of their information.[155] In the event of a breach, users may lose faith in a system and seek to take their business elsewhere. Like other areas of the GDPR, this can create both technical and legal problems that hinder the continued development and implementation of AI-based network defense systems. Moving forward, these challenges are only likely to be compounded as AI technologies move towards greater autonomy.

B. TRAINING AI-BASED NETWORK DEFENSE SYSTEMS AND AUTOMATED INFORMATION SHARING: TODAY'S COMPLIANCE AND TOMORROW'S OUTLOOK

The GDPR aims to protect consumers by regulating the processing of personal data.[156] As described above, the development and use of AI-based network defense systems cannot escape the breadth of this regulation.[157] On the front end, the development of these systems requires data to foster the machine learning process.[158] Systems need personal data such as usernames, IP addresses, and other cyber threat indicators to train systems on normal behavior and empower systems to identify malicious activity.[159] Once these systems are in place,

---

153. *See* Humerick, *supra* note 108, at 409 ("[T]he right to portability poses similar problems to those inherent in the rights to consent and erasure.").

154. *See* Buckner, *supra* note 97 ("If an AI system is well constituted and trained, has algorithms for prediction evaluation, and demonstrably produces reasonably high quality, true positive results, then that model may be suited for its purpose.").

155. *See Cybersecurity, AI, and Machine Learning: The Connection to GDPR*, TREND MIRCO (Apr. 26, 2018), https://www.trendmicro.com/vinfo/pl/security/news/security-technology/cybersecurity-ai-and-machine-learning-the-connection-to-gdpr ("Under GDPR, cybersecurity companies are mandated to obtain explicit consent and explain to customers how their data will be processed by security engines that use AI technology.").

156. *See* GDPR, art. 1(1).

157. *Supra* Part II, Section A.

158. *See, e.g.*, *Artificial Intelligence for a Smarter Kind of Cybersecurity*, IBM, https://www.ibm.com/security/artificial-intelligence (last visited Feb. 9, 2020) (indicating that AI is trained by "consuming billions of data artifacts").

159. *Cf.* Nathan McKinley, *The Promise and Challenges of AI and Machine Learning for Cybersecurity*, COP MAGAZINE (Nov. 28, 2019), https://www.cpomagazine.com/cyber-security/the-promise-and-challenges-of-

they still require continuous data to learn in a dynamic threat environment.[160] Moreover, the success of these systems moving forward will be heavily dependent on the ability to act at cyber speed.[161] This can only be achieved when networks and systems are constantly sharing information, and AI will likely be a solution to this end.[162] While this may be an ideal scenario for cybersecurity, it also brings network defense further within the scope of the GDPR.[163] This section examines the larger challenges of GDPR compliance associated with training algorithms and information sharing. This leads into a broader discussion in Section C regarding the dichotomy of autonomous network defense and the challenges of cybersecurity as these systems become more automated and capable of autonomous action.

1. Training AI-Based Network Defense Systems

Good data drives good systems. Generally, AI systems that train using machine learning processes require large quantities of good data to produce successful results, and network defense is no different. As discussed in Part I, AI-based network defense is primarily driven by machine learning approaches that enable intrusion detection through signature and anomaly-based techniques.[164] The breadth of relevant data can be vast. Network activity, such as routing information and user activity, allows an AI system to characterize network traffic and establish a more effective baseline that can be used to identify potentially

---

ai-and-machine-learning-for-cybersecurity/ (explaining that "without relevant datasets, you just cannot evaluate the security risks and threats at all").

160. *See id*.

161. *See id*. ("Timely detection of the security threat or dangerous malware is the key to gain a competitive and proactive lead in providing security safeguards.").

162. *See, e.g.*, Derek Manky, *AI and Machine Learning Will Have Significant Impact on Cyber Security Strategies*, INFO. MGMT. (Jan. 9, 2020, 3:30 AM), https://www.information-management.com/opinion/ai-and-machine-learning-will-have-significant-impact-on-cybersecurity-strategies (proposing that future AI cybersecurity systems for will require vastly more sophisticated information-sharing capabilities).

163. *See* Cybersecurity, AI, and Machine Learning: The Connection to GDPR, *supra* note 155 (indicating that cybersecurity companies will need to implement additional measures around collecting and processing personal data to meet compliance requirements of the GDPR).

164. *See Supra* Part I.

malicious deviations.[165] Similarly, large quantities of malware samples and other cyber threat intelligence information enables these systems to identify external threats in a dynamic threat environment.[166] This collectively promotes a more effective system capable of identifying and combatting malicious cyber activity.

As discussed in Section A, the GDPR places significant restrictions on how data is collected and used.[167] In a sense, it can be thought of as an availability problem. Will the GDPR impose enough restrictions on the availability of good data to the point where the development and implementation of these systems may be unjustly stunted?[168] At a minimum, this will require entities that develop or implement AI-based cybersecurity solutions to rethink approaches to collecting and securing data. Like other areas of technology, this can prove challenging when there is a gap in knowledge between technology and the law.[169] Moreover, transparency issues associated with AI, such as the black box problem, may make this an insurmountable task in some instances.[170] It is not to say that the requirements of the GDPR cannot be overcome, but it will likely require extensive resources to maintain compliance. From consent procedures to technical safeguards, developers and users of AI-based network defense systems will be required to reevaluate procedures and practices to comply with the data

---

165. *See* Mustafa Rassiwala, *Network Traffic Analytics—Do We Need One More Network Security Category?*, LASTLINE (Oct. 25, 2018), https://www.lastline.com/blog/network-traffic-analytics-do-we-need-one-more-network-security-category/ (explaining AI applications in the field of network traffic analytics).

166. *See* Darek Manky, *Threat Intelligence Lies at the Core of All Machine Learning and AI*, FORTINET (Oct. 8, 2019), https://www.fortinet.com/blog/industry-trends/threat-intelligence-at-the-core-ai-machine-learning.html (discussing the need for good threat intelligence in order to detect today's cybersecurity threats).

167. *See supra* Part II, Section A.

168. *See* Ahmed Baladi, *Can GDPR Hinder AI Made in Europe,* CYBERSECURITY L. REP. (July 10, 2019) https://www.gibsondunn.com/wp-content/uploads/2019/07/Baladi-Can-GDPR-Hinder-AI-Made-in-Europe-Cybersecurity-Law-Report-10-07-19.pdf.

169. *See, e.g.*, Gijs Leenders, *The Regulation of Artificial Intelligence—A Case Study of the Partnership on AI*, MEDIUM (Apr. 13, 2019), https://becominghuman.ai/the-regulation-of-artificial-intelligence-a-case-study-of-the-partnership-on-ai-c1c22526c19f (arguing that regulators and the law tend to lag behind technology and innovation).

170. *See supra* Part I, Section C.

collection, consent, automation, and explanation requirements of the GDPR.[171] In practice, only time will tell how significant the impact of the GDPR on the development of network defense systems that use AI technologies may be. Notwithstanding, there are some foreseeable consequences in this regard.

First, it is likely that the GDPR will favor larger entities that have the resources to navigate compliance and employ cutting-edge technologies. From legal expertise to the use of advanced systems, large companies will be in the best position to implement safeguards to ensure compliance. Second, smaller companies may be most affected by this regulation in terms of developing AI-based solutions to network security. Innovation in this domain often comes from niche companies that develop narrow cybersecurity applications. It will become increasingly hard for these developers to independently find good data sets and to apply appropriate methods for compliance. Lastly, this could have a collective impact on the network defense market. The cybersecurity industry is increasingly turning to AI-based solutions. However, additional restrictions could shift the economic utility of advanced systems as research and development becomes more costly. The restrictions could also cause those entities with less resources to defer the use of AI-based cybersecurity solutions.

Despite these foreseeable consequences, it is important to note that regulation is not a zero-sum game. The GDPR will likely have some impact on the development and proliferation of AI-based cybersecurity systems; however, it is also unlikely that it will completely inhibit research and development in this field. In some respects, the GDPR may enhance autonomous cybersecurity. The GDPR is a data protection and data governance regulation.[172] No matter where one stands on the spectrum of its utility, there is likely value in the GDPR as a tool to promote awareness of cybersecurity issues. While there may be other avenues to promote awareness, the GDPR has nonetheless forced issues surrounding privacy and security to the forefront of business considerations. At the heart of data

---

171. *See Cybersecurity, AI, and Machine Learning: The Connection to GDPR*, *supra* note 155 (proposing that the tech industry, including cybersecurity companies implementing AI, will need to "retool" products and services to adapt to the GDPR era).

172. *See* Layton & Mclendon, *supra* note 124, at 235 (suggesting that the GDPR is a data protection measure; not a privacy regulation).

protection is the use of technical systems and such heightened awareness could promote investment in data security systems. As in many areas of law and technology, the only certainty is often uncertainty and only time will tell how significant of an impact the GDPR has on the development of AI and cybersecurity.

2. Automated Information Sharing

Often, the value of information is limited by the extent to which it can be shared. A known cyber threat indicator may be useful to the entity that has it, but its value can quickly diminish when other systems or entities are in the dark. As discussed in Part I, information sharing of indicators and cyber threat intelligence is a significant component of network defense. This sharing can take many forms. Network defense systems can automatically distribute information across systems and networks, just as ISACs and other cyber threat sharing entities can share a spectrum of relevant threat information. The GDPR, in the interest of data protection, prescribes rules for information sharing surrounding consent, explanation requirements, and automated processes. However, it does not fully hinder the exchange of information. In fact, portions of the GDPR encourage sharing information related to network and information security.[173]

Recital 49 of the GDPR notes that data controllers have a legitimate interest in the "processing of personal data to the extent strictly necessary and proportionate for the purpose of ensuring network and information security."[174] This recital specifically identifies computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs), as well as other public authorities and providers of security technologies and services that would be considered data controllers. Essentially, this encourages authorized information sharing entities to share information that includes personal data when they have a legitimate interest and when doing so is necessary and proportionate to ensure network and information

---

173. *See Information Sharing and Cooperation Enabled by the GDPR*, MISP (Jan. 30, 2018), https://www.misp-project.org/compliance/gdpr/information_sharing_and_cooperation_gdpr.html ("Recital 49 of the GDPR confirms that CSIRTs [computer security incident response teams] are encouraged to share information . . . .").

174. GDPR, Recital 49.

security.[175] Although this is a recital, and not an enforceable regulation, it suggests that the GDPR is not meant to inhibit cyber threat information sharing.[176] This concept is supported by Article 32, which notes that controllers and processors "shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk . . . ."[177] In the cybersecurity domain, information sharing is critical to protecting data and is therefore likely to be considered an essential measure to lowering risk.[178]

Although sharing of information is permitted, it is still restricted by the GDPR. As noted, processing of data must be necessary and proportional for the purpose of network and information security. This most certainly creates some legal uncertainty. What is necessary and proportionate for an ISAC may be different for other parties in the cyber threat community, such as network defense system vendors. Further, it raises questions as to what is necessary and proportional, how this determination is made, and by whom. The first place to look at what could be necessary and proportional is the GDPR itself; in particular, the principles set forth in Article 5 (lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; and integrity and confidentiality).[179] Article 6(1)(e) also provides some guidance in this regard.[180] It notes that "processing shall be lawful only if and to the extent that . . . [it] is necessary for the performance of a task carried out in the public interest or in the exercise of

---

175. *Information Sharing and Cooperation Enabled by the GDPR*, *supra* note 173.

176. *Id.*

177. GDPR, art. 32.

178. *Information Sharing and Cooperation Enabled by the GDPR*, *supra* note 173 ("Information has to be perceived as [an] essential security measure to lower the risk.").

179. GDPR, art. 5; *see also Information Sharing and Cooperation Enabled by the GDPR*, *supra* note 173 (noting that a processing activity should comply with the six principles set forth in Article 5 of the GDPR).

180. *See* GDPR, art. 6(1)(e) ("Processing shall be lawful only if and to the extent that at least one of the following applies: [. . .] (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller . . . ."); *see also Information Sharing and Cooperation Enabled by the GDPR*, *supra* note 173 (suggesting that the legality of processing activities for CSIRTs may be based on Article 6(1)(e) of the GDPR).

official authority vested in the controller."[181] This is in no way definitive, as there remains ambiguity in what may be in the public interest and who may exercise official authority. However, it supports the idea that the GDPR was in no way meant to fully inhibit information sharing; rather, it seeks to regulate how it may be done.

Similar to the development of AI-based cybersecurity systems, only time will tell how significant the impact of the GDPR may be on cyber threat information sharing. Increased regulation will warrant a greater investment in technologies and expertise to ensure compliance. However, it is in no way a foregone conclusion that this would materially alter the course of AI in the cybersecurity domain. A key consideration at this point, is how information is actually shared. As noted in Part I, network defense systems that are advertised as AI-driven still require a significant level of human control. This means there are analysts behind information sharing decisions who can strip shareable data of personal data in the interest of compliance. Although these processes are becoming more automated, there is human control nonetheless. Moving forward, the demands of an increased and dynamic threat landscape will require faster decision-making and more automation. As AI-based cybersecurity systems shift towards greater autonomy, they will be more capable of meeting these demands but may also create more questions for compliance.

C. THE AUTONOMY PROBLEM: WHEN DOES AI BREAK THE MOLD?

Regardless of the domain, a common question for legal scholars examining AI is whether AI will break the mold. Put differently, when does AI make traditional legal regimes obsolete? For example, autonomous driving vehicles may someday disrupt traditional liability regimes related to strict liability and negligence.[182] The very nature of AI and the black box problem could prevent the legal system from determining whether there was a breach of duty, who was responsible, and whether the breach caused the damage. This has required

---

181. GDPR, art. 6(1)(e).

182. *See generally* U.S. CHAMBER INSTITUTE FOR LEGAL REFORM, TORTS OF THE FUTURE: AUTONOMOUS VEHICLES 3–6 (2018) (addressing the liability and regulatory implications for autonomous vehicles).

engineers and legal teams to rethink the foundational principles of AI technologies.[183] It also begs the question, when does AI break the mold, if at all, for cybersecurity and data protection?

As noted in Part I, AI-based network defense systems are still primarily detect-and-respond tools that require significant human intervention.[184] As they stand, these systems primarily assist network defenders in analyzing data and making connections to determine the context and nature of network activity.[185] The fact that there remain significant levels of human control, as discussed in Section B, supports the idea that compliance, although challenging, may be possible in today's system.[186] GDPR compliance may hinder or slow progress, but there are no indications that it will fully inhibit the development and use of AI-based network defense systems. Notwithstanding, there should be serious concern moving forward as to whether compliance is feasible as the underlying technologies move towards greater autonomy.

Ideally, these systems will be able to one day operate at "cyber" speed. In fact, they may have to as malicious actors and cyber criminals increasingly utilize AI to further nefarious activity.[187] The future may very well be a battle of algorithms where competing systems act and react with little or no human intervention. In terms of the GDPR, the question becomes whether compliance is still feasible in the wake of greater autonomy. The black box problem is just one example of an area where compliance may be unachievable.[188] The right to an explanation holds little weight when an explanation is not possible. This will require system developers to look for technological solutions that promote transparency from the beginning. Similarly, in the context of cyber threat information

---

183. *See generally* Buckner, *supra* note 97 (answering questions pertaining to how engineers and legal teams must change their thinking about growing AI technologies).

184. *Supra* Part I, Section B.

185. *See* Marty, *supra* note 60 (describing how machine learning algorithms reveal security insights, safeguard data, and keep attackers out of systems).

186. *Supra* Part I, Section B.

187. *See* Danny Palmer, *AI, Quantum Computing and 5G Could Make Criminals More Dangerous Than Ever, Warn Police*, ZDNET (July 19, 2019), https://www.zdnet.com/article/ai-quantum-computing-and-5g-could-make-criminals-more-dangerous-than-ever-warn-police/ (describing how AI can aid criminals in exploiting vulnerable IoT devices).

188. *Supra* Part I, Section B.

sharing, fully autonomous systems may excel at communicating cyber threat information across systems and entities but may also be incapable of demonstrating that personal data was not shared. As suggested earlier, the only certainty is uncertainty.[189] Absent innovative technologies that can assure protected data is processed in accordance with regulations like the GDPR, it is likely that AI-based cybersecurity systems will break the mold. Moving forward, it is incumbent on engineers, lawmakers, and scholars in their respective fields to pursue technology and policies that balance the demands of cybersecurity with the need to protect data.

For AI and cybersecurity, the problem space is immense, and the implications are likely to be significant. The demands of information security are often at odds with data privacy.[190] Meanwhile, rapid transformations in the threat landscape and changes in technology make it difficult to understand the broader picture of these competing domains.[191] This poses challenges for all parties involved trying to balance respective interests and move society forward in the most effective fashion. If done correctly, a balanced regulatory scheme may be able to minimize data privacy issues in cybersecurity while prompting the overall development and implementation of autonomous information security systems.

D. ENGINEERING POLICY: CONSIDERATIONS FOR THE FUTURE OF AUTONOMOUS CYBERSECURITY

Technology almost always outpaces the law. As technology builds upon technology, governing mechanisms often struggle to understand and account for the regulatory, ethical, and privacy considerations surrounding emerging technologies. Moreover, a lack of understanding of the technology itself often makes formulating policy difficult. Technology often not only outpaces our ability to defend but also our will to do so. AI is no exception. From the Internet to cybersecurity to big data and AI, there are

---

189. *See* Tegmark, *supra* note 3 (noting that "the boundaries of AI can be uncertain and have tended to shift over time").

190. *See generally* Danny Guaman, *Software and Services Engineering: Privacy vs. Data Protection vs. Information Security*, STRAST, https://blogs.upm.es/sse/2016/11/01/privacy-vs-data-protection-vs-information-security/ (last visited Feb. 22, 2020) (discussing the differences between information security and data privacy).

191. *See id*.

intrinsic considerations related to data rights, privacy, intellectual property, ethics, due process, social values, and geopolitical concerns. Converging technologies complicate regulatory structures at all levels. While the law is lost in the fog of innovation, society struggles to harmonize the social challenges presented by such disruptive technologies. For machine learning and information security, the public puts a premium on privacy while still expecting the benefits of AI systems where the utility is derived from surpluses of consumer data.[192]

Data privacy, or rather data protection, has received significant attention in the wake of weekly large-scale data breaches. This has caused technology firms and regulators to warm to the idea of federal privacy legislation.[193] In the interest of cybersecurity and AI, there are several key considerations for a federal privacy statute that may drive the future of autonomous network defense. First, a federal privacy law may benefit from certain exemptions for data processing related to information security.[194] This could include exemptions that permit automated sharing of cyber threat indicators so long as information is shared by approved or vetted systems or entities. A second consideration is the inclusion of liability limitations for small companies. While these exemptions would need to be uniquely tailored so as to not to defeat the purpose of the legislation, such exemptions would encourage smaller vendors and companies to employ more advanced systems.[195] Depending on the state of the technology, the proliferation of more advanced

---

192. *See generally* April F. Doss, *Why Changes in Data Science Are Driving a Need for Quantum Law and Policy, and How We Get There*, 14 ABA SCITECH LAW. 38, 40 (2017).

193. *See generally* Dan Clark, *Federal Data Privacy Legislation Is Likely Next Year, Tech Lawyers Say*, LAW.COM (Nov. 29, 2018), https://www.law.com/corpcounsel/2018/11/29/federal-data-privacy-legislation-is-likely-next-year-tech-lawyers-say/ (detailing how tech companies and regulators are releasing their own opinions on what data privacy legislation should consist of).

194. *See* Nick Wallace & Daniel Castro, *The Impact of the EU's New Data Protection Regulation on AI* at 5, CTR. FOR DATA INNOVATION (Mar. 27, 2018), http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf (suggesting that the GDPR exempts certain forms of data processing when doing so is in the public interest and that national governments should use this authority).

195. *Id*. at 3 (noting that smaller firms subject to the GDPR would be less likely to adopt AI technologies because of the disproportionality associated with fines under the regulation).

systems may benefit the cybersecurity industry as a whole and shift the economics of cybersecurity in a positive fashion.

Another consideration would be to outline permitted uses of anonymized[196] and pseudonymized data.[197] Because achieving full anonymization of data can be challenging, entities may be hesitant to use or share such information. Outlining permitted uses of anonymized and pseudonymized data would reduce uncertainty surrounding information sharing by clearly establishing instances where anonymized data sharing is appropriate. This would, however, also likely require standardization of certain data anonymization techniques. A similar consideration would be to define permitted uses of repurposed data without additional consent.[198] In some instances, it is foreseeable that relevant information may be collected for a particular purpose but may be useful at a later time when the threat landscape has changed. Defining when it would be permissible to repurpose this data without additional consent would enable respective network defense entities to more rapidly respond to a threat.

CONCLUSION

Breakthroughs in the development of AI technologies continuously shift the application of AI from a conceptual dream to a tangible reality. As each technological advancement is reduced to practice, questions of law and policy surrounding AI become more complex and convoluted. In the context of information security, AI offers a spectrum of utility ranging from

---

196. *See* GDPR, Recital 26 ("To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.").

197. See GDPR art.4, (5) ("For the purposes of this Regulation . . . (5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person . . . ."); *see also* Wallace & Castro, *supra* note 194 (suggesting that the EU should revise the right to erasure so that companies are callable of deleting or anonymizing data in ways that do not impact the underlying algorithms).

198. *See* Wallace & Castro, *supra* note 194 (suggesting that the EU should amend the GDPR to allow for personal data to be repurposed without additional consent).

automation that empowers analysts to protect a network to systems capable of thinking, learning, and acting in a manner more intelligent than humans. As the threat landscape expands, society is turning towards AI systems to combat growing cyber threats. Meanwhile, society struggles to harmonize data privacy concerns with technological realities. The GDPR has brought this discussion to the pinnacle of business considerations by regulating how data is to be protected. In today's infant state, AI-based cybersecurity systems appear capable of tackling the challenge of compliance. However, the challenge becomes more difficult as these systems achieve greater autonomy. As the cybersecurity industry moves forward, it is paramount that engineers, legal experts, and society look to balance competing interests in cybersecurity and data privacy in order to realize the benefits afforded by AI technologies.