**This month’s OSINT focus is:**

**ARTIFICIAL INTELLIGENCE**

**What is artificial intelligence (best definition)?**

Artificial intelligence (AI) is the theory and development of computer software and hardware systems capable of performing tasks that historically required human intelligence, such as recognizing speech, making decisions, and identifying patterns.

The first comment about Artificial Intelligence, which is frequently just called AI, is that it is a misnomer. The power and impact of AI in today’s world, and tomorrow’s world, is so powerful that it should really be called “Stupendous Intelligence,” or “Super Intelligence,” which is more appropriate. AI has already had enormous impact on our lives and many parts of our society

At its roots, AI is the software that inhales huge amounts of data, compares the data ingested, and spits out one or more results. It requires huge amounts of data so that the huge amounts data acquired can be compared and bad data ignored. We are just not talking about a dozen, or hundreds, or thousands, but millions, or more, amounts of related data. The AI software learns from comparing huge amounts of like data and learns and draws conclusions based on analyzing all data accumulated for analysis. When there are only small amounts of data available, the AI conclusions are not reliable, and should not be used.

Humans also learn by comparing data, but we usually only need small amounts of data to make conclusions. We also have eyes and ears that gather data. Our brains do not require huge amounts of data to draw conclusions, and the capabilities of individual brains vary from person to person, as some people learn much faster than other people. We rely on our eyes to gather a lot of data and lead us to conclusions.

Today, there is a lot of evidence that AI is everywhere. Ai and Automation (robots) are affecting all our lives. AI is part of the process of eliminating jobs. Initially AI has replaced humans in jobs that require repetitive effort, as machines using AI can perform tasks faster and more reliably than humans. A business owner greatly benefits when AI controlled robots perform repetitive tasks faster and more reliable than humans. AI robots do not need to rest and can work 24 hours – when necessary. The robots need to be properly maintained, but AI software can track robots and perform maintenance when breakdown is predicted or detected. Monitoring active robots, it can detect and predict when maintenance is needed, to prevent breakdowns. This gives factories the capability to function 24 hours a day and indefinitely.

The operations in a company like Amazon, which must receive online orders 24 hours a day and then provide service 24 hours a day to receive, sort and store, millions of products, and then access and distribute stored products 24 hours a day, then deliver products to customers within 24 hours nationally, can only be operational and effective with AI automated operations.

AI and robots are now impacting education including robot teachers, robots for physical security of school buildings and even robots to fend off shooters to protect students, teachers, and school staff. This first generation of robots can quickly call 911 but can only disrupt shooters by positioning their metal bodies between the shooter and human targets. The next generation of school robots may be able to disable a shooter, or other type of trouble-maker.

Robots used for teaching will provide consistent course content so that lower income students attending convenient local schools get a quality education to prepare them for colleges and universities.

AI and robots are already augmenting fire fighters as the robots can initially enter a building, or any location that is on fire, and provide a picture of the situation to give firefighters with sufficient information to deal with the emergency effectively. They can also get closer to the fire to disperse water or retardant. They can also assist in taking victims away from the fire situation.

AI and robots are used in some police organizations to initially approach a situation scanning for information to locate and protect victims, or potential victims, and locate any suspect(s) to strategize the resources and tactics needed to neutralize the suspect(s).

Robots can be used to teach firefighters and police officers different training topics. Controlled training taught by robots provides training that is consistent and approved as competent and necessary by management.

Robots are used in medicine to prov needed routine services such as the distribution of medicine for many patients which is more effectively done by robots controlled by computers that insure that accurate medication is always provided to patients with a glass of water to take pills. This simple task is not easily and accurately accomplished by human beings.

Robots are used to conduct actual operations (sometimes managed by doctors), or assist some doctors conducting operations.

In Las Vegas, robots are doing bartending working long shifts and other robots provide food service to gamblers and guests in their rooms or on next to a slot machine.

Today, anyone calling up a medical organization for an appointment, or calling your bank for service, or your local police, or most government offices, or your insurance company will be greeted by a robot. Owners like robots because they are always available, provide consistent information to the public, and save money by reducing manpower. Robots do not get overtime pay, vacations, retirement income, childcare expenses, healthcare expenses, locker rooms, bathrooms, and meal facilities. They don’t need meals and won’t sue their bosses. They also do not complain.

Management effort and staffing can be reduced as many personnel costs go away with the reduction of human staff. Robots do not get salaries, vacation, retirement planning, sick pay, health insurance, which reduces eliminates time and effort.

The McKinsey Global Institute forecasts that automation will force as many as 70 million workers in the United States to find new skills, or find another way to generate income by 2036. (Source: “Robots could replace nearly a third of the U.S. Workforce by 2030” Danielle Paquette, Washington Post, Nov 30, 2017.)

**AI and National Security**

The use of AI in national security is a huge issue with many opportunities for good and bad. In the past, the major nations that had the biggest guns, or biggest bombs that could be used against an opponent would be the winner. Guns and bombs are not irrelevant, but if one nation can stop another nation from using bullets or bombs, that would be the ultimate **coup**.

AI offers this opportunity. If one nation can stop another nation from employing traditional methods to kill their enemy, they will be the winner. The most potent power for any major nation is to be able to disable their opponent’s ability is to prevent their opponent from delivering munitions (warheads, conventional and/or nuclear).

Can the possession of superior AI skills determine the winner in a major conflict?

Communications has been, and will be a key component in warfare. If one nation can seriously disrupt, or destroy their opponent’s primary communications capabilities, they can prevent their opponent from conducting offensive attacks. That doesn’t mean the missiles, airplanes, and/or submarines would cease operations. But if communications can be disrupted or destroyed, accurate targeting will not be possible.

Recall that in the last 5 years, both the Russians and the Chinese have been practicing destroying satellites (and creating a mess with debris). The Chinese also have been attempting to physically manipulate satellites with physical extensions. Our opponents know that if they can disrupt or destroy our communications satellites, we will not be able to communicate with our ground troops, aircraft, missiles or submarines, or guided missile destroyers.

Satellites provide intelligence on the location of the enemy, their size and weapons. They provide midcourse and final course guidance for our long-range missiles, bombers, and missiles launched from submarines and our guided missile vessels.

We are aware of these threats, but can only hope and pray that our strategic planners can counter the threats that our enemies are planning on employing.

For our Air Force, our Space Command has a huge and challenging mission, and this Command must be funded and skillful personnel recruited for this holy mission.

Recommend that serious readers read the November/December 2023 issue of Foreign Affairs magazine for the article “ AI Is Already at War,” by former US Undersecretary of Defense for Policy, Michelle Flournoy, pp 56-69.

Ms. Flournoy explains the importance of AI in any future conflict, especially with China which has focused huge funding to AI research.

The US Department of Defense and our Air Force, Navy and Army are all gearing up AI technologies to fight the next super war with China, not the Russians. Unfortunately, we are underfunded, and need money to support all the projects we need to employ to win any future conflict that utilizes AI technology. AI requirements are already impacting many aspects of our military, including the dire need for additional qualified personnel, new digital organizations that need both funding and competent personnel, and fiscal support from Congress. You can review this report as it is attached.

President Biden’s staff saw this report briefed him on the contents.

On October 30, 2023, after his staff’s briefing, President Biden was so impressed that he immediately signed a sweeping executive order to guide the development of artificial intelligence. The order will require industry to develop safety and security standards, introduce new consumer protections and give federal agencies an extensive to-do list to oversee the rapidly progressing technology.

More amazingly, two days later, on November 1, 2023, China joined the U.S, UK, and the nations in the EU declaring AI very dangerous. China signed the declaration, which included the sentence: “We welcome the international community’s efforts so far to cooperate on AI to promote inclusive economic growth, sustainable development and innovation, to protect human rights and fundamental freedoms, and to foster public trust and confidence in AI systems to fully realize their potential.”

Dr Fei Fei Li, the Chinese American heroine we introduced in our October 2023 Post newsletter was featured in a full-page article “Fei Fei,” Wall Street Journal, Nov 4, 2023.

We noted last month that she was focused on AI and Medicine. In this article she warns that AI cannot be left to be driven in the private sector, which is motivated primarily by profit. Given the power of the technology, she says it’s too dangerous to let big tech companies regulate themselves. Innovation is needed in these challenging times, our lawmakers must regulate AI without killing innovation.

Finally, perfectly illustrating how one dangerous capability of AI to manipulate reality, by altering imagery, including motion imagery can be harmful and most dangerous.

On the front page of the Wall St Journal, 4 Nov 2023, we read that “**Fake Nudes of Teens Shake a School”.** One person(s) at Westfield High School in New Jersey, used AI technology and pasted the images of female nude bodies attached to the head shots of many female students. There were even images of people performing sexual behavior.

Welcome to the 23rd Century and the fact that we can no longer believe what we see. Our eyes, which we have all used to confirm reality, can no longer be trusted to show us the truth.

============================================================

**SOURCES:**

**AI Is Already at War**

**How Artificial Intelligence Will Transform the Military**

**Michèle A. Flournoy, *Foreign Affairs*, November/December 2023, Oct 24, 2023**

In 2002, a special operations team practiced raiding a safehouse. The team silently approached a two-story building, built for military training, where a fictitious terrorist leader was hiding. One soldier crept up to an open window and tossed in a small drone piloted by artificial intelligence. The AI drone began flying autonomously through the building, room by room, beaming footage from its camera directly to the commander’s handheld tablet outside. In just a few minutes, the team had full situational awareness of the interior of the building. It knew which rooms were empty, which were occupied by sleeping family members, and where the primary target was. The team entered the building knowing exactly where to go, reducing the risk for each member. The drill was a success: had it been real, the team would have killed the terrorist leader.

The AI-piloted quadcopter, designed by Shield AI (where I was an adviser), has since been used in real-world operations. It is just one of the many ways that AI is beginning to reshape U.S. national security. The U.S. military is using AI to optimize everything from equipment maintenance to budgetary decisions. Intelligence analysts are relying on AI to quickly scan mountains of information to identify relevant patterns that enable them to make better judgments and to make them faster. In the future, Americans can expect AI to change how the United States and its adversaries fight on the battlefield, as well. In short, AI has sparked a security revolution—one that is just starting to unfold.

As AI has burst into the public consciousness, some researchers, worried about AI’s dangers, have called for a pause on development. But stopping American AI progress is impossible: the mathematical foundations of AI are ubiquitous, the human skills to create AI models have widely proliferated, and the drivers of AI research and development—both human creativity and commercial gain—are very powerful. Trying to stop progress would also be a mistake. China is working hard to surpass the United States in AI, particularly when it comes to military applications. If it succeeds, Beijing would then possess a much more powerful military, one potentially able to increase the tempo and effect of its operations beyond what the United States can match. China’s ability to use cyber and electronic warfare against U.S. networks and critical infrastructure would also be dangerously enhanced. Put simply, the Pentagon needs to accelerate—not slow—its adoption of responsible AI. If it doesn’t, Washington could lose the military superiority that underwrites the interests of the United States, the security of its allies and partners, and the rules-based international order.

Acceleration, however, is easier said than done. The United States may lead the world when it comes to artificial intelligence research and development, but the U.S. government still struggles to adopt innovative technologies such as AI with speed and at scale. It does not employ enough professionals with the technical expertise needed to test, evaluate, procure, and manage AI products. It is still building the data and computer infrastructure necessary to support large AI models. It lacks the flexible funding required to quickly take the most promising AI prototypes and scale them across agencies. And it has yet to build up the testing and evaluation processes and platforms needed to ensure that any AI integrated into military systems is safe, secure, and trusted. When AI plays a role in the use of force, the bar for safety and reliability must remain very high.

Politicians and defense officials are aware of these issues. Congressional leaders are paying close attention to AI, and they are discussing how they can regulate the industry and yet keep it globally competitive. The Office of the Secretary of Defense has issued a policy framework for AI to expedite its responsible and safe adoption by the Defense Department. The essential effort to simultaneously foster AI and put guardrails around its use—aims that are seemingly in tension—is underway.

But Congress has yet to act, and the implementation of the Pentagon’s AI framework is still very much a work in progress. Although the creation of a Chief Digital and Artificial Intelligence Office at the Defense Department was an important milestone, Congress has yet to provide this office with the resources it needs to drive responsible AI adoption across the defense establishment. To ensure that AI defense applications are both safe and successful, the Pentagon will need to further bolster AI guardrails, add new technical staff, and develop new ways of testing and procuring AI. Time is of the essence, and the stakes are too high for the United States to fall behind.

HERE AND NOW

Even as policies and regulations are still being written, AI is already transforming U.S. security. The U.S. Air Force, for example, is beginning to use AI to help it allocate resources and to predict how a single decision can reshape its program and budget. If air force leaders, for example, add another squadron of F-35s, their AI-enabled resource allocation platform can immediately highlight not only the direct costs of the decision but also its effects on personnel, bases, aircraft availability, and other important domains.

Similarly, the military is beginning to use AI models in the maintenance of complex weapons systems, from ships to fighter jets. AI programs can now collect data from a platform’s sensors and predict when and what kind of maintenance will maximize its readiness and longevity while minimizing costs.

These maintenance insights are tremendously helpful, and they are just the beginning of what predictive AI can do. The U.S. intelligence community and several U.S. combatant commands—the joint military commands with operational responsibility for a particular region or function—are using AI to sift through reams of classified and unclassified data to identify patterns of behavior and forecast future international events. In the intelligence community, AI helped analysts predict Russia’s invasion of Ukraine months in advance, enabling the United States to warn the world and deny Russian President Vladimir Putin the element of surprise. At U.S. Strategic Command, AI developed by Rhombus Power (where I am an adviser) is being used to help warn officials about the movement of nuclear-armed missiles that often evaded detection in the past.

Predictive AI could also give Washington a better understanding of what its potential adversaries might be thinking, especially leaders in Beijing. Unlike during the height of the Cold War, when there were legions of experts on Soviet decision-making, the United States is still figuring out how China’s leadership translates policy into specific actions. The intelligence community could, for instance, develop a large language model that would ingest all available writings and speeches by Chinese leaders, as well as U.S. intelligence reports about these figures, and then emulate how Chinese President Xi Jinping might decide to execute stated policy. Analysts could ask the model specific questions—“Under what circumstances would President Xi be willing to use force against Taiwan?”—and anticipate potential responses based on a wealth of data from more sources than any human being could ever quickly synthesize. They could even ask the model to map out how a crisis might unfold and how different decisions would shape the outcome. The resulting insights could be useful in informing analysts and policymakers, provided the training sets were transparent (meaning they cite the sources of data underlying key judgments) and trusted (not prone to “hallucinations”—inexplicable inferences made by AI).

AI has sparked a security revolution that is just starting to unfold.

Intelligence officers are already using AI daily to sift through thousands of pictures and videos. In the past, analysts had to watch thousands of hours of full-motion video to find and tag objects of interest, whether a concentration of tanks or dispersed mobile missiles. But with AI, developers can train a model to examine all this material and identify only the objects the analyst is looking for—usually in a matter of seconds or minutes. The analyst can also set the AI model to send an alert whenever a new object of interest is found in a given geographic area. These “computer vision” tools enable analysts to spend more time doing what only humans can do: applying their expertise and judgment to assess the meaning and implications of what AI discovers. As these models become more accurate and trusted, they have the potential to help U.S. commanders on the ground make critical operational decisions much faster than an adversary can respond, giving U.S. forces a tremendous—perhaps even decisive—advantage.

AI could support military operations in other ways, as well. For instance, if an adversary were to jam or attack U.S. command, control, and communications networks, AI could enable a smart switching and routing agent that would redirect the flow of information between sensors, decision-makers, and shooters to make sure they stay connected and can maintain situational awareness. Having these capabilities will be critical to ensuring that Washington and its allies can make better decisions faster than their adversaries, even in the thick of combat.

AI could further help U.S. and allied forces by amplifying the work of individual service members in the field. Some AI applications currently in development allow a single human operator to control multiple unmanned systems, such as a swarm of drones in the air, on the water, or undersea. For example, a fighter pilot could use a swarm of flying drones to confuse or overwhelm an adversary’s radar and air defense system. A submarine commander could use undersea unmanned vehicles to conduct reconnaissance in a heavily defended area or to hunt for undersea mines that threaten U.S. and allied ships. The Pentagon recently announced its Replicator drone program, which promises to field thousands of small, smart, low-cost, expendable, autonomous systems within the next two years.

In a conflict with China over Taiwan, this human-machine teaming could be critical. If Beijing decides to use force to claim the island, China will have the advantage of fighting in its own backyard, allowing it to mass forces more easily. The United States, meanwhile, will be sending its units long distances and in far fewer numbers. If the U.S. military can augment its manned platforms such as fighters, bombers, ships, and submarines with large numbers of relatively cheap unmanned systems, it could compensate somewhat for this comparative disadvantage and greatly complicate the Chinese military’s operations.

PLAY IT RIGHT

Beijing, of course, has no intention of ceding technological dominance to Washington. It is working hard to develop its own advanced AI military applications. China is investing heavily in many of the same AI use cases as the United States—such as surveillance, target identification, and drone swarms. The difference is that it may not be bound by the same ethical constraints as the United States and its allies, particularly when it comes to using fully autonomous weapons systems.

In the race for technological supremacy, China has some obvious advantages. Unlike Washington, Beijing can dictate its country’s economic priorities and allocate whatever resources it deems necessary to meet AI targets. China’s national security policy encourages Chinese hackers, officials, and employees to steal Western intellectual property, and Beijing is unabashed in trying to recruit leading Western technologists to work with Chinese institutions. Because China has a policy of “civil-military fusion,” which eliminates barriers between its civilian and military sectors, the People’s Liberation Army can draw on the work of Chinese experts and companies whenever it likes. And by 2025, China will churn out nearly twice as many Ph.D. candidates in science, technology, engineering, and mathematics as the United States does, flooding China’s economy with talented computer scientists in particular.

But the United States has its own unique strengths. The country’s market-based economy and more open political system give developers room to be creative. It has unrivaled innovation ecosystems in Silicon Valley, the Austin metropolitan area, the Massachusetts Route 128 corridor, and elsewhere. The United States also has a vibrant venture capital and private equity ecosystem that draws incomparable domestic and international investment. It is home to many of the world’s leading universities, allowing it to attract and retain some of the world’s best tech talent. Indeed, half the startups in Silicon Valley have at least one founder who is an immigrant. Even among those who lament China’s rapid AI progress, few, if any, would trade the United States’ hand for China’s. But almost all of them would agree the United States needs to play its hand better to win.

To do so, the Defense Department and the intelligence community will have to invest more in accelerating AI adoption. They can start by building common digital infrastructure systems that share the same standards to ensure interoperability. The infrastructure would include cloud-based technologies and services; common data standards; validated data sets; shared access to secure software stacks; sophisticated tools for the testing, evaluation, and validation of AI models; and secure application programming interfaces that control who gets access to what information at various levels of classification. The goal would be to give developers the data, algorithms, tools, and compute power—or high-speed computing power—they need to create, test, validate, and use new AI tools.

Those tools will only be as good as the people who operate them, of course, and right now, the Defense Department does not have a digitally adept workforce. Few people on staff understand enough about AI to properly govern its use, to test and evaluate AI tools to ensure they meet the Pentagon’s “responsible AI” standards, or to assess which AI models best meet the needs of the military or the Defense Department—one of the world’s largest enterprises.

To attract more AI talent and to make better use of the tech workforce it already has, the Defense Department will need to improve how it recruits and manages digitally skilled employees. The Pentagon can start by following the advice of the National Security Commission on AI and establish a digital corps (modeled on the Army Medical Corps) to organize, train, and equip technologists. In addition, all the existing military service academies should start teaching the basics of AI, and the Pentagon should also establish a U.S. digital service academy that would educate and train aspiring civilian technologists, offering them a free college education in exchange for a commitment to serve in government for at least five years after graduating. Finally, the Defense Department should create a digital reserve corps in which tech workers from across the United States could volunteer, part time, to serve their country.

The Pentagon, however, will never be able to attract as many AI experts as the private sector. The defense establishment must therefore improve how it leverages outside talent. For starters, the Defense Department should deepen its conversations with technology companies and the computer science departments of leading universities. It should also reduce some of the outdated barriers to tech firms doing business with the government. To do so, defense officials must rethink how they buy software-based products and services, including AI. Instead of taking years to develop a fixed set of highly specific requirements—as the department does when procuring military hardware—it should quickly identify the specific problems it is trying to solve and the common standards that any proposed solutions must meet and then allow companies to offer solutions in a competitive bidding process. It should also make sure that the people who will actually use the specific AI tools are able to provide feedback as models are being developed and tested.

In fact, the Pentagon should create a dedicated career path for acquisition professionals who want to specialize in AI and other commercially driven technologies. Most of the Defense Department’s current acquisition corps have been trained to buy complex weapons systems, such as submarines, missiles, and jets, which requires paying meticulous attention to whether contractors meet rigid specifications, cost requirements, and scheduled milestones. As a result, most of these professionals are (understandably) highly risk averse—they are neither trained nor incentivized to buy rapidly developing commercial technologies or to disrupt an existing multiyear acquisition program to integrate a more effective new technology. The Pentagon should therefore create a new cohort of acquisition experts who are specifically trained to buy these kinds of systems. This cadre should be considered the Green Berets of the acquisition force, and its members should be rewarded and promoted based on their ability to quickly deliver and scale needed commercial technologies, such as AI.

Beijing has no intention of ceding technological dominance to Washington.

Although internal reforms will help the Pentagon accelerate progress, defense officials will also need sustained congressional support to keep pace with their Chinese counterparts. To that end, Congress should give the Defense Department more flexible funding that allows it to optimally manage AI programs. Most of the Pentagon’s appropriations are fixed: when Congress funds a program, the department cannot simply redirect the money to something else. But AI is evolving so fast, and in so many different directions, that defense officials need more reprogramming authorities and more flexible funding so they can quickly move money out of underperforming projects and reinvest it in more promising ones, giving Congress appropriate notice. This approach is critical to enabling the Pentagon to adopt AI with more agility and speed.

Congress should simultaneously provide the Chief Digital and Artificial Intelligence Office with bridge funding to help promising AI pilot projects cross the so-called valley of death—the difficult period between when a project demonstrates success and when the department is ready to make it a full-scale program of record. The U.S. military simply cannot afford to delay the adoption of a critical AI tool that emerges in 2023 until the 2025 budget or later.

The United States will also need to continue attracting the best tech talent in the world, including by reforming elements of the U.S. immigration system. Science and technology students and workers may want to come to and stay in the United States, but byzantine immigration rules make it impossible for many of them to do so. Educational visas, for instance, do not let foreign students stay in the United States for more than three years after graduation. The resulting dynamic is perverse: U.S. institutions train many of the world’s best tech experts, only to send them away. Many of them are Chinese and return to China.

In addition, congressionally imposed caps on H-1B visas—the visa the United States most commonly offers to skilled workers—mean that the country can bring in only a small percentage of people who apply. For example, from the 758,994 eligible electronic registrations received during the 2023 H-1B lottery, only 110,791 people were selected (or less than 15 percent). In short, the United States is keeping out much-needed foreign talent that would willingly and meaningfully contribute to the country’s ability to compete in AI and other critical technologies.

HIGH RISK, HIGH REWARD

AI is indispensable to the United States’ future security. But it also poses major risks. AI is already accelerating the spread of disinformation online and facilitating inadvertent discrimination in hiring. Computer scientists have argued that it could enable automated cyberattacks at “machine speeds,” as well. Chemists have shown that AI can synthesize chemical weapons, and biologists have expressed concern that it could be used to design new pathogens or bioweapons. The risks are severe enough that even AI industry leaders have expressed alarm. In May 2023, the heads of almost every major U.S. AI lab signed a letter warning that their inventions could pose an existential threat to humanity.

Indeed, national security is the realm of human activity where the risks of AI are most profound. AI models could, for example, misidentify people or objects as targets, resulting in unintended death and destruction during conflict. Black box AI models—ones whose reasoning cannot be adequately understood or explained—might lead military planners to make hazardous decisions. This risk would be most acute if AI developed for one situation were applied to another without enough testing and oversight. What might be perfectly rational and responsible in one situation might be irrational and dangerous in another.

The risks do not stem just from poorly designed or carelessly used systems. The United States could be fastidious in developing and implementing AI, only for its adversaries to find ways to corrupt U.S. data, prompting systems to go haywire. For example, if an adversary were able to spoof an AI-enabled computer vision tool into targeting a civilian vehicle instead of a military one, it could cause the United States to inadvertently harm civilians in a conflict zone, undermining U.S. credibility and moral authority. An adversary could also corrupt data in ways that would degrade the performance of an AI-enabled weapon system or that could cause it to shut down.

The Pentagon is aware of these risks, and in February 2020, it issued a set of ethical principles governing how AI should be used. One principle called on the department’s personnel to exercise judgment and care in developing, deploying, and using AI capabilities. Another said the Defense Department will try to “minimize unintended bias in AI capabilities.” A third called for ensuring that all AI is made and used in ways that can be understood and explained—with data and methodologies that are transparent and auditable. And defense leaders have directed their employees to make sure that AI systems are rigorously tested for their safety, security, and effectiveness; that AI systems are assigned to clearly defined uses; and that AI systems can be disengaged or deactivated if they exhibit unintended behavior.

 For autonomous and semiautonomous weapons, the Defense Department has issued even more specific guidance. Pentagon leaders have directed commanders and operators to use careful judgment over AI-enabled weapons, including by ensuring that these weapons are used in ways that are consistent with the parameters of the model’s training and with the rules of engagement for the operation in which the AI is being deployed. The Defense Department’s rules also stipulate that commanders use AI in accordance with the laws of war. For example, any AI-enabled weapon must be discriminate, able to distinguish between combatants and noncombatants on the battlefield, and able to avoid deliberately targeting the latter. The Pentagon has also forbidden the use of AI in its nuclear command-and-control systems, and it has urged other nuclear powers to do the same.

Among the U.S. defense community’s leadership, these “responsible AI” rules have achieved great consensus. But putting them into practice is no small challenge—especially given the size of the United States’ defense apparatus. The Pentagon has started the process by creating a high-level governance body, beginning to establish data and digital infrastructure to support a variety of AI applications; building out the testing, evaluation, and validation capabilities needed to ensure compliance with the Defense Department’s AI principles; and increasing AI awareness across the department. This implementation process is still in its infancy. But the policy framework provides a sound basis on which to build.

Still, the Pentagon would be wise to further strengthen these guidelines. For example, defense officials should require that all AI vendors give the Defense Department full transparency into the origins of data they use in their training sets. In addition, the department should make sure that the behavior of any AI model it adopts is explainable (fully understood by its users and developers), without stifling innovation. It can do so by strengthening how it tests, evaluates, and verifies systems. The department should also scale and broaden the work done by the Defense Advanced Research Projects Agency—one of the entities responsible for developing emerging technologies for the military—on making sure that AI tools are explainable and responsible by design. The department’s ethical principles, in other words, should be treated as required traits that shape how defense AI models are designed from the start.

U.S. institutions train many of the world’s best tech experts, only to send them away.

But the U.S. defense community will not be able to speed AI adoption unless the public believes it will use AI in ways that are effective, responsible, ethical, and lawful. Otherwise, the first time an AI application leads to a very bad decision or serious unintended consequences on the battlefield, warfighters are unlikely to trust it, and policymakers and lawmakers are likely to suspend or prohibit its use. The Defense Department must therefore increase its investment in the research and development of AI safety and security. It must be transparent about what it will and will not use AI to do. And the Pentagon should consider making its vendors put guardrails on how they develop AI. If a company wants to provide AI to the military, for example, the Defense Department could require it to meet rigorous data protection and cybersecurity standards. By doing so, the Pentagon could help make AI safer, not just for the armed forces, but for everyone.

The United States, of course, cannot singlehandedly make sure that AI is developed and used responsibly. Other countries—including competitors—will also have to adopt policy guardrails and norms. The world took a valuable first step when, in November 2021, 193 countries approved a global agreement on the ethics of artificial intelligence—the world’s first. It includes the principle that countries must guarantee human oversight of and agency over all AI.

Although this agreement is an important foundation, the United States should seek out venues to discuss AI with its potential adversaries, especially China, just as it found ways to talk about nuclear weapons and other forms of arms control with the Soviet Union during the Cold War. To succeed, Washington will also have to work closely with its allies and partners to make sure they are all on the same page. Countries that agree on a set of AI norms should be willing to threaten violators with severe costs, including multilateral economic sanctions, expulsion from international forums, and legal action to hold perpetrators responsible for damage. Actors that violate AI rules, for instance, could be indicted in a U.S. federal court, as five Chinese hackers were in 2014 for launching cyberattacks on U.S. companies. States that violate these rules could face potential retaliation for any harm done—including, in extreme cases, military action.

THE NEED FOR RESPONSIBLE SPEED

In the world of microelectronics, experts often talk about Moore’s law: the principle that the number of transistors on chips doubles every two years, resulting in exponentially more capable devices. The law helps explain the rapid rise of so many technological innovations, including smartphones and search engines.

Within national security, AI progress has created another kind of Moore’s law. Whichever military first masters organizing, incorporating, and institutionalizing the use of data and AI into its operations in the coming years will reap exponential advances, giving it remarkable advantages over its foes. The first adopter of AI at scale is likely to have a faster decision cycle and better information on which to base decisions. Its networks are likely to be more resilient when under attack, preserving its ability to maintain situational awareness, defend its forces, engage targets effectively, and protect the integrity of its command, control, and communications. It will also be able to control swarms of unmanned systems in the air, on the water, and under the sea to confuse and overwhelm an adversary. The United States cannot afford to fall behind.

But the national security apparatus cannot afford to be reckless, either. Without proper safeguards, AI models could cause all kinds of unintended harm. Rogue systems could even kill U.S. troops or unarmed civilians in or near areas of combat. The United States therefore finds itself facing a conundrum. The stakes of slowing AI down are unacceptably high, but so are the stakes of racing ahead without needed precautions.

U.S. policymakers appear to understand this paradox. Congressional leaders know that if they were to regulate AI with too heavy a hand, they could prompt the best AI innovators to leave the United States to work where there are fewer restrictions, and the United States would then fall behind its competitors. But both Democratic and Republican policymakers also know that some regulation and oversight is essential to ensuring that AI adoption is safe and responsible. The House of Representatives and the Senate are holding sessions to educate their members and scheduling hearings to get advice from experts. These efforts to build bipartisan consensus before legislating should be applauded.

Yet understanding the problem is just the first step. To solve it—to balance the need for speed with the need for safety—policymakers will have to implement better approaches to accelerating adoption as well as ensuring safety. Otherwise, Americans risk being caught in a world of both spiraling AI dangers and declining U.S. power and influence.

============================================================

**Biden wants to move fast on AI safeguards and signs an executive order to address his concerns**

**JOSH BOAK and MATT O'BRIEN, *Associated Press* •October 30, 2023**

 **WASHINGTON (AP)** — President Joe Biden on Monday signed an ambitious executive order on artificial intelligence that seeks to balance the needs of cutting-edge technology companies with national security and consumer rights, creating an early set of guardrails that could be fortified by legislation and global agreements.

Before signing the order, Biden said AI is driving change at “warp speed” and carries tremendous potential as well as perils.

“AI is all around us,” Biden said. “To realize the promise of AI and avoid the risk, we need to govern this technology.”

The order is an initial step that is meant to ensure that AI is trustworthy and helpful, rather than deceptive and destructive. The order — which will likely need to be augmented by congressional action — seeks to steer how AI is developed so that companies can profit without putting public safety in jeopardy.

Using the Defense Production Act, the order requires leading AI developers to share safety test results and other information with the government. The National Institute of Standards and Technology is to create standards to ensure AI tools are safe and secure before public release.

The Commerce Department is to issue guidance to label and watermark AI-generated content to help differentiate between authentic interactions and those generated by software. The extensive order touches on matters of privacy, civil rights, consumer protections, scientific research and worker rights.

In Biden's view, the government was late to address the risks of social media and now U.S. youth are grappling with related mental health issues. AI has the positive ability to accelerate cancer research, model the impacts of climate change, boost economic output and improve government services among other benefits. But it could also warp basic notions of truth with false images, deepen racial and social inequalities and provide a tool to scammers and criminals.

With the European Union nearing final passage of a sweeping law to rein in AI harms and Congress still in the early stages of debating safeguards, the Biden administration is “stepping up to use the levers it can control,” said digital rights advocate Alexandra Reeve Givens, president of the Center for Democracy & Technology. "That’s issuing guidance and standards to shape private sector behavior and leading by example in the federal government’s own use of AI.”

The order builds on voluntary commitments already made by technology companies. It's part of a broader strategy that administration officials say also includes congressional legislation and international diplomacy, a sign of the disruptions already caused by the introduction of new AI tools such as ChatGPT that can generate text, images and sounds.

Biden on Monday, Oct. 30, will sign a sweeping executive order to guide the development of artificial intelligence. The order will require industry to develop safety and security standards, introduce new consumer protections and give federal agencies an extensive to-do list to oversee the rapidly progressing technology. (AP Photo/Michael Dwyer, File)© Provided by The Associated Press

The guidance within the order is to be implemented and fulfilled over the range of 90 days to 365 days.

Last Thursday, Biden gathered his aides in the Oval Office to review and finalize the executive order, a 30-minute meeting that stretched to 70 minutes, despite other pressing matters, including the mass shooting in Maine, the Israel-Hamas war and the selection of a new House speaker.

Biden was profoundly curious about the technology in the months of meetings that led up to drafting the order. His science advisory council focused on AI at two meetings and his Cabinet discussed it at two meetings. The president also pressed tech executives and civil society advocates about the technology's capabilities at multiple gatherings.

“He was as impressed and alarmed as anyone,” deputy White House chief of staff Bruce Reed said in an interview. “He saw fake AI images of himself, of his dog. He saw how it can make bad poetry. And he’s seen and heard the incredible and terrifying technology of voice cloning, which can take three seconds of your voice and turn it into an entire fake conversation.”

The issue of AI was seemingly inescapable for Biden. At Camp David one weekend, he relaxed by watching the Tom Cruise film “Mission: Impossible — Dead Reckoning Part One.” The film's villain is a sentient and rogue AI known as “the Entity” that sinks a submarine and kills its crew in the movie's opening minutes.

“If he hadn’t already been concerned about what could go wrong with AI before that movie, he saw plenty more to worry about,” said Reed, who watched the film with the president.

Governments around the world have raced to establish protections, some of them tougher than Biden's directives. After more than two years of deliberation, the EU is putting the final touches on a comprehensive set of regulations that targets the riskiest applications with the tightest restrictions. China, a key AI rival to the U.S., has also set some rules.

U.K. Prime Minister Rishi Sunak hopes to carve out a prominent role for Britain as an AI safety hub at a summit starting Wednesday that Vice President Kamala Harris plans to attend. And on Monday, officials from the Group of Seven major industrial nations agreed to a set of AI safety principles and a voluntary code of conduct for AI developers.

The U.S., particularly its West Coast, is home to many of the leading developers of cutting-edge AI technology, including tech giants Google, Meta and Microsoft, and AI-focused startups such as OpenAI, maker of ChatGPT. The White House took advantage of that industry weight earlier this year when it secured commitments from those companies to implement safety mechanisms as they build new AI models.

But the White House also faced significant pressure from Democratic allies, including labor and civil rights groups, to make sure its policies reflected their concerns about AI’s real-world harms.

Suresh Venkatasubramanian, a former Biden administration official who helped craft principles for approaching AI, said one of the biggest challenges within the federal government has been what to do about law enforcement’s use of AI tools, including at U.S. borders.

“These are all places where we know that the use of automation is very problematic, with facial recognition, drone technology,” Venkatasubramanian said. Facial recognition technology has been shown to perform unevenly across racial groups, and has been tied to mistaken arrests.

While the EU’s forthcoming AI law is set to ban real-time facial recognition in public, Biden’s order appears to simply ask for federal agencies to review how they’re using AI in the criminal justice system, falling short of the stronger language sought by some activists.

The American Civil Liberties Union is among the groups that met with the White House to try to ensure “we’re holding the tech industry and tech billionaires accountable” so that algorithmic tools “work for all of us and not just a few,” said ReNika Moore, director of the ACLU’s racial justice program, who attended Monday's signing.

After seeing the text of the order, Moore applauded how it addressed discrimination and other AI harms in workplaces and housing, but said the administration “essentially kicks the can down the road” in protecting people from law enforcement’s growing use of the technology.

=========================================================

**UK, US, EU and China sign declaration of AI’s ‘catastrophic’ danger**

**Bletchley summit communique does not agree to set up testing hub in UK, as some in government had hoped**

Kiran Stacey and Dan Milmo, the Guardian, Wed 1 Nov 2023

The UK, US, EU, Australia and China have all agreed that artificial intelligence poses a potentially catastrophic risk to humanity, in the first international declaration to deal with the fast-emerging technology.

Twenty-eight governments signed up to the so-called Bletchley declaration on the first day of the AI safety summit, hosted by the British government. The countries agreed to work together on AI safety research, even amid signs that the US and UK are competing to take the lead over developing new regulations.

Rishi Sunak welcomed the declaration, calling it “quite incredible”.

In remarks ahead of his own appearance at the summit on Thursday, the prime minister added: “There will be nothing more transformative to the futures of our children and grandchildren than technological advances like AI.

“We owe it to them to ensure AI develops in a safe and responsible way, gripping the risks it poses early enough in the process.”

How AI chatbots like ChatGPT or Bard work – visual explainer

Referring to the risks posed by the most advanced AI systems, the declaration stated: “There is potential for serious, even catastrophic, harm, either deliberate or unintentional, stemming from the most significant capabilities of these AI models.”

Michelle Donelan, the UK technology secretary, told reporters: “For the first time we now have countries agreeing that we need to look not just independently but collectively at the risks around frontier AI.”

Frontier AI refers to the most cutting-edge systems, which some experts believe could become more intelligent than people at a range of tasks. Speaking to the PA news agency on the sidelines of the summit, Elon Musk, the owner Tesla and SpaceX, and of X, formerly Twitter, warned: “For the first time, we have a situation where there’s something that is going to be far smarter than the smartest human … it’s not clear to me we can actually control such a thing.”

The communique marks a diplomatic success for the UK and for Sunak in particular, who decided to host the summit this summer after becoming concerned with the way in which AI models were advancing rapidly without oversight.

Donelan opened the summit by telling her fellow participants that the development of AI “can’t be left to chance or neglect or to private actors alone”.

She was joined onstage by the US commerce secretary, Gina Raimondo, and the Chinese vice-minister of science and technology, Wu Zhaohui, in a rare show of global unity.

Matt Clifford, one of the British officials in charge of organising the summit, called the appearance of Raimondo and Wu together on stage “a remarkable moment”.

**China signed the declaration, which included the sentence: “We welcome the international community’s efforts so far to cooperate on AI to promote inclusive economic growth, sustainable development and innovation, to protect human rights and fundamental freedoms, and to foster public trust and confidence in AI systems to fully realise their potential.”**

Wu told fellow delegates: “We uphold the principles of mutual respect, equality and mutual benefits. Countries regardless of their size and scale have equal rights to develop and use AI.”

South Korea has agreed to host another such summit in six months’ time, while France will host one in a year.

So far, however, there is little international agreement over what a global set of AI regulations might look like or who should draw them up.

Some British officials had hoped other countries would agree to beef up the government’s AI taskforce so that it could be used to test new models from around the world before they are released to the public.

Instead, Raimondo used the summit to announce a separate American AI Safety Institute within thecountry’s National Institute of Standards and Technology, which she called “a neutral third party to develop best-in-class standards”, adding that the institute would develop its own rules for safety, security and testing.

Earlier this week, the Biden administration released an executive order requiring US AI companies such as OpenAI and Google to share their safety test results with the government before releasing AI models.

Kamala Harris, the vice-president, then gave a speech on AI in London in which she talked about the importance of regulating existing AI models as well as more advanced ones in the future.

Clifford denied any suggestion of a split between the US and UK on which country should take the global lead on AI regulation.

“You’ll have heard Secretary Raimondo really praise us in a full-throated way and talk about the partnership that she wants to have between the UK and the US safety institute,” he said. “I really think that that shows the depth of the partnership.”

Sunak said the summit had proved “the appetite from all of those people for the UK to take a leadership role”.

The EU is in the process of passing an AI bill, which aims to develop a set of principles for regulation, as well as bringing in rules for specific technologies such as live facial recognition.

Donelan suggested the government would not include an AI bill in the king’s speech next week, saying: “We need to properly understand the problem before we apply the solutions.”

But she denied the UK was falling behind its international counterparts, adding: “We have called the world together – the first ever global summit on AI at the frontier – and we shouldn’t minimize or overlook that.”

============================================================

**Fei-Fei**

***CAYCE CLIFFORD, The Wall Street Journal* | Page C014, 4 November 2023**

****

**The AI pioneer thinks the technology is too powerful to leave entirely to the private sector.**

Fei-Fei Li, a renowned pioneer in artificial intelligence, says a conversation with her mother changed the course of her career. She notes that her parents, who brought her to the U.S. from China when she was 15 with hopes for a better life, had always been supportive of her work. But about a decade ago her mother asked: “Fei-Fei, what exactly do you *do?”*

As Li writes in her new memoir, “The Worlds I See: Curiosity, Exploration, and Discovery at the Dawn of AI,” Li, 47, explained how her interest in the “mysteries of intelligence” spurred her to create a massive data set of images to teach computers how to identify objects in the world. That feat is now widely credited with helping to spawn the “deep learning” revolution in AI. Her mom was intrigued but unmoved. “What,” she pointedly asked, “can AI do to help people?”

The question was unexpectedly humbling, and Li says it pushed her to see AI as a tool, not just a concept. Now, as a computer science professor at Stanford University and co-director of its Institute for Human-Centered Artificial Intelligence, which she helped found in 2019, Li is calling for both innovations that improve people’s lives and better safeguards against AI’s dangers. Those include, she says, the spread of disinformation, the threat to jobs posed by automation and the rise of algorithms with inherent biases against nonwhite, nonmale users.

“As we create more and more powerful technology, we need to make sure we are not just exacerbating intolerance, exacerbating unfairness,” Li says from her office at Stanford. She is troubled that most AI products are managed by the private sector, and universities and other nonprofits can no longer afford to build the kind of aspirational, problem-solving technology she hopes to see. “Not a single university in America has the resources to train ChatGPT,” she says, referring to the popular chatbot created by OpenAI, which got a $10 billion infusion from Microsoft in January. In September, Amazon announced it would invest up to $4 billion in Anthropic, a rival to OpenAI.

Li has been calling for federal investment in AI research by academics and nonprofits, and welcomes President Biden’s recent executive order, which she believes will “catalyze AI innovation” by including such funding. She wants to see Congress enshrine such resources into law. She argues that the power of AI to both create and solve big problems is too great to relinquish its development to the wealthiest private companies. “AI can really help us find a cure for cancer, it can help to superpower our teachers, it can help us map out biodiversity,” she says. “But we could miss these discoveries if diverse voices aren’t at the table.”

Li credits her own unconventional background with inspiring her interest in using AI to improve healthcare. “Having taken care of immigrant parents who don’t speak English, and for many years didn’t have the means to have health insurance, I have some insights that maybe a technologist from an affluent background would never have,” she says. In partnership with Stanford Medical School and Hospitals, Li and her students are figuring out how AI can improve hospital hygiene, relieve staff of tasks, and improve patient safety. Given that medical errors are a top cause of U.S. deaths, and the industry suffers from high burnout rates, “this is an area where a lot of help is needed,” she says.

Growing up in Chengdu, Li sensed that her life lay elsewhere. Despite the claims of some of her teachers that boys were “biologically smarter” than girls, she was a top student, fascinated, she says, by the poetry and “grandeur” of physics. When she and her parents secured U.S. visas and moved into a cramped one-bedroom apartment in Parsippany, N.J. in 1992, she felt buoyed by the fact that Albert Einstein had been an immigrant, too.

At Princeton University, she balanced her studies with helping her parents run their dry-cleaning shop. Her interest in physics gave way to computers, which she believed could decode and even model the workings of the human mind. “I was inspired by asking audacious questions about the universe, like, ‘What is intelligence?’” she says. As a doctoral candidate at the California Institute of Technology, Li began exploring how the brain processes what it sees, guided by a hunch that teaching visual comprehension to machines could be key to creating artificial intelligence. (She also met Silvio Savarese, a fellow grad student in computer science, now her husband and the father of their two children.)

Against a “chorus of detractors,” she writes, Li began categorizing images for a huge database to teach vision to computers. At Stanford, where she was invited to bring her lab in 2009, she unveiled ImageNet, a repository of 15 million images across 22,000 categories. It got little attention - until 2012, when an algorithm trained on this data was able to identify previously unfamiliar pictures 85% of the time, surpassing all prior efforts. By 2015 a machine trained on ImageNet could beat the human error rate of 5.1%.

By then, interest in AI had moved beyond academia into Silicon Valley, with some disturbing results. In 2015, Google and Yahoo algorithms notoriously mislabeled photos of Black people as “gorillas” and an “ape,” respectively, which highlighted some of the perils of relying on data sets and algorithms that were created mainly by white men. “If the people behind a

As AI’s power grows, ‘We need to make sure we are not just exacerbating intolerance, exacerbating unfairness.’

product’s design and decision-making come from only one angle, we’re going to miss a lot,” says Li.

She promptly helped found what would become AI4ALL, a nonprofit that aims to increase diversity and inclusion in AI, with funding from Melinda French Gates and Nvidia founder Jensen Huang. “If we’re not cultivating the curiosity and talents of children from every background, we might just miss incredible human capital,” says Li, who says she has often felt lonely as a rare woman in a field dominated by men.

Her 21-month spell as chief scientist of AI at Google Cloud, while on sabbatical from Stanford in 2017 and 2018, drove home what Li calls “the messiness of this technology.” She says her time at the center of a controversy over a Google Cloud contract with the Defense Department, which spurred some employees to resign over the potential for AI tools to be used to target lethal drone strikes, felt like “a coming-of-age moment” for AI. Amid growing public concerns over flawed facial-recognition software, self-driving-car deaths and threats to privacy, Li decided it was time for a new framework for thinking about these problems, which she branded “human-centered AI.”

From her lab, which brings together economists, sociologists, political scientists, physicists, and others to better understand AI’s effects, Li says she is cautiously hopeful that lawmakers will figure out how to regulate AI without killing innovation. Given the power of the technology, she says it’s too dangerous to let big tech companies regulate themselves. “If you’re taking a pill, do you want to know that the FDA has conducted randomized trials to test its effectiveness?” she asks. “Or do you want to just believe the company when it says it’s safe?”

===============================================

**Fake Nudes of Teens Shake a School**

**The Wall Street Journal | Page A001, 4 November 2023**

When girls at Westfield High School in New Jersey found out boys were sharing nude photos of them in group chats, they were shocked, and not only because it was an invasion of privacy. The images weren’t real.

Students said one or more classmates used an online tool powered by artificial intelligence to make the images, then shared them with others. The discovery has sparked uproar in Westfield, an affluent town outside New York City.

Digitally altered or faked images and videos have exploded along with the availability of free or cheap AI tools. The lack of clarity on such images’ legality— and how or whether to punish their makers—has parents, schools and law enforcement running to catch up as AI speeds ahead.

The high school confirmed the incident in an email to parents, but a Westfield Public Schools spokeswoman declined to provide details on the number of students involved or to confirm any disciplinary action, citing student confidentiality.

Some Westfield parents said their daughters have felt humiliated and powerless and worry about damage to the girls should the images surface later. And they are upset that no resolution is forthcoming.

Even among parents, there is no consensus. In a local Facebook group, some called for harsh punishment for whoever created the images. Others deemed it a youthful transgression that should be forgiven. Westfield police are investigating, and a state senator has asked county prosecutors to look into the case.

Sophomore boys at West-field High were acting “weird” on Monday, Oct. 16, whispering among themselves and being quieter than normal, said one mom, recounting what her daughter, a classmate, told her.

Girls started asking questions, the mom said. Four days later, one boy told some of the girls what all the whispering was about: At least one student had used an AI-powered website to make pornographic images using girls’ photos found online, then shared them with other boys in group chats. Girls at Westfield reported the situation to school administrators, who began interviewing boys who might have known more information.

In an Oct. 20 email to parents, Westfield High Principal Mary Asfendis said she believed the images had been deleted and weren’t being circulated. “This is a very serious incident,” Asfendis wrote. “New technologies have made it possible to falsify images and students need to know the impact and damage those actions can cause to others.” She pledged to continue teaching children about responsible technology use.

Several girls were told by school administrators that some boys had identified them in the generated images, according to parents. The district spokeswoman declined to say whether school staff members had reviewed the images.

The girls’ parents who spoke to The Wall Street Journal—including two of the four who filed reports with police—said they and their daughters hadn’t seen the images. Police haven’t seen them either, according to a person familiar with the investigation.

“To be in a situation where you see young girls traumatized at a vulnerable stage of their lives is hard to witness,” Westfield Mayor Shelley Brindle said in an interview. Brindle encourages people affected by this situation to give statements to the police. A spokeswoman for the town of West-field said the police department wouldn’t comment.

Dorota Mani said her 14year-old daughter, Francesca, was told by the school that her photo was used.

“I am terrified by how this is going to surface and when. My daughter has a bright future, and no one can guarantee this won’t impact her professionally, academically, or socially,” said Mani, who has filed a police report.

While people have been able to doctor images with Photo-shop and similar software for years, new AI image- makers make it easy to produce entirely fabricated photos.

“You would have needed an entire cluster of computers to generate images a few years ago. “Now you just need an iPhone,” said Ben Colman, CEO of Reality Defender, which works with companies and government to detect Ai generated fake images.

Image generators from big companies—like OpenAI’s Dall-E and Adobe’s Firefly—have moderation settings that bar users from creating pornographic images. But a quick online search turns up dozens of results for face-swapping and “clothes removing” tools. Because these services likely use publicly available software, moderation and technical guardrails are difficult, if not impossible, to enforce and implement, Colman said. It is almost impossible for the human eye to distinguish real from fake, he added.

More than 90% of such false imagery—known as “deepfakes”— are porn, according to image-detection firm Sensity AI.

Faked sexual images of real people are so new, federal law is lagging, say legal experts. A handful of states, including Virginia, California, Minnesota, and New York, have outlawed the distribution of faked porn, or given victims the right to sue its creators in civil court.

Jon Bramnick, a New Jersey state senator who represents Westfield, is co-sponsoring a bill to criminalize the dissemination of such material. “This has to be a serious crime in New Jersey,” he said, adding that he has asked the Union County prosecutor to investigate.

Laws covering child sexual-abuse material could apply in this situation, said Natalie Elizaroff, an intellectual-property lawyer in Chicago, because they prohibit digital images, computer images or even computer- generated images of minors engaged in sexually explicit conduct.

At a meeting at her home Monday, Mani’s daughter, Francesca, described what she and other Westfield High girls are going through. “At first I cried, and then I decided I should not be sad,” she told the group. “I should be mad and should advocate for myself and the other victims.”

Among the attendees were parents of other students, along with Brindle, Bramnick, three female town-council members and a school-board member. (The Journal was invited to listen in by phone.)

At a group counseling session at school that day, some girls had said they were uncomfortable having to attend school with someone they believed had created and shared the images, Francesca said.

The incident has made some of her female classmates’ rethink what they post online, she said. Some, she said, deleted their social-media accounts.

“We’re aware that there are creepy guys out there,” she told the group, “but you’d never think one of your classmates would violate you like this.”

==========================================================