AI and Data Privacy Protection: Recognizing Fears, Appreciating Benefits

SUMMARY
Artificial Intelligence is the latest technology to move into the "Trough of Disillusionment" of Gartner's Hype Cycle—the phase where negative press, skepticism, and public paranoia is at its peak. The culprit for all this negativity comes from the fear surrounding the proliferation of personal data, accessed by AI programs, and its vulnerability to misuse.

Four key sources of threat include:

Social Media and Digital Marketing
Facebook's controversial data oversharing has many social media users questioning how much of their data is being sold or manipulated. One journalist downloaded his data file from Google and found it included almost 3 million Word documents full of intimate personal information.

In the Workplace
More than 40% of worldwide employers use artificial intelligence processes of some kind, including for monitoring employee activities. Few laws govern what data can be collected at work and how it can be used.

Healthcare
About 86% of healthcare provider organizations and technology vendors apply artificial intelligence technology. Personal medical information in the marketplace is believed to be 10 times higher than credit card data, which makes data theft irresistible to cybercriminals.

Human Rights
Often, the collection and creation of databases necessary for AI to work are used — with or without bad intentions — to make assumptions about people. Regardless of intent, many see these practices as an interruption of the fundamental rights to privacy and data protection.

So how do we protect unapproved access and handling of people's data?

Some responses include:

- **Data Encryption, Masking & Containerization**
- **Data Use Verification**
- **Universal Regulations / Guidelines**
  - *(The EU's GDPR is an experiment to watch)*
- **Use AI to Combat Data Fraud**
- **Use Humans as Gatekeepers**
- **But First … Educate, Earn Trust, Gain Consent**

In this paper, we dig deeper into these topics, their implications, and seek to balance the real societal fears with the overwhelming benefits of AI technology. While threats to data privacy are real, we'll explain how these fears should not stop us from adopting its innovations.

INTRODUCTION

The use of Artificial Intelligence (AI), machine learning, and Robotic Process Automation has exploded in recent years. In 2017 alone companies spent around $22 billon on AI-related mergers and acquisitions, around 26 times more than in 2015. In fact, many dubbed 2017 as "The Year of AI."

While it's commonly associated with self-driving cars, digital assistants, and Netflix recommendations, AI is used ubiquitously throughout almost every industry and increasingly in most everyday tasks. Consultant group McKinsey Global Institute believes that just applying AI to marketing, sales, and supply chains could create over $2.7 trillion in economic value over the next 20 years.[1]

Mostly used to collect, comb through, analyze, and interpret large amounts of data (much more than a human could, and faster), AI has become more valuable as more data has become available. Machine learning relies on vast amounts of data to recognize patterns. With the advent of the internet and cloud technologies, sources of data and its collection have increased. Vulnerabilities for data theft or misuse of information have increased with it.

"AI requires a ton of data, so the privacy implications are bigger," says Andras Cser, vice president and principal analyst at Forrester Research. "There's potential for a lot more personally identifiable data being collected."[2]

The rise in threats means data security has become essential at every step of AI technology implementation. What makes these threats so intimidating is how deep they can impact people's lives. Crimes are not limited to losing material wealth. With cybercrime, identity thieves fraudulently apply for loans, ruin credit through online shopping sprees, and digital insurance fraud.

"Identity theft historically involved stealing credit card numbers and racking up large bills," says Dr. Gokul Solai, CEO of AI firm Novation Solutions. "But data theft now goes even deeper."

"When criminals steal your personal health data, the impact is more so than just monetary," continues Solai. "Now it's like stalking — like in movies when hackers can know everything about you and ruin your life. We all know about the conventional threats, but the unknown is what's so scary."

What's even more scary is the pace at which personal data cybercrime is spreading.

"We have seen identity fraud attempts increase year-on-year, now reaching epidemic levels, with identities being stolen at a rate of almost 500 a day," says Simon Dukes, chief executive of fraud prevention organization Cifas.[3]

In the UK, the Cyber Security Breaches Survey 2017 revealed that almost half of all businesses identified at least one cybersecurity attack in the last year. Among medium-sized (66%) and large organizations (68%), the threat is even more substantial.[4]

It's easy to see why consumers continue to fear AI with dangers like these. According to a Genpact survey, most people are still uncomfortable with their personal information being used, even if it means a better experience with companies.[4]

- Almost 75% say they don't want companies to use AI if means infringing on their privacy
- Only 6% say they are comfortable with personal data being used to customize their user experience
- 63% are concerned AI will make choices that impact them without their knowledge
- 59% think governments should do more to protect consumers' personal data from AI
- 55% of those ages 55+ don't see the personal benefit of AI
- 71% of consumers fear AI will infringe on their personal privacy in some way

“I can understand why people would be skeptical of AI,” says Solai. “There’s a sense of pessimism that we have to overcome. It all comes from expecting the worst. And with cybercriminals, the worst-case scenario is using your data to manipulate your very behavior.”

Since AI is now so pervasive, worst case scenarios like behavior manipulation can seem around every corner. But what arenas are the most threatening? Here are four that rise to the top, including an optimistic counterpoint by Dr. Solai (to help us overcome the inevitable paranoia).

SOURCES OF THREAT

Social Media and Digital Marketing

In 2014, researchers from political data firm Cambridge Analytica asked users to take a personality survey and download an app. This survey scraped private information from their profiles and those of their friends — including details on users' identities, friend networks, and "likes."

Later hired by President Trump's 2016 election campaign, Cambridge Analytica harvested data from 50 million Facebook users through access given to them by the social media platform. Only the 270,000 from the app download had consented to sharing their information. This personal information was later used to target ads toward the users and their network.

The Cambridge Analytica incident has shed new light on how social media platforms collect and share user data with third parties, especially companies that spend millions of ad dollars targeting their users. Many social media platforms get information from apps and websites that use their services (ads, "share" and "like" buttons, analytics services, account logins). Included participants like Twitter, Pinterest, LinkedIn, Amazon, Google, and Facebook make up some of the most visited, widely-used services on the internet.

According to a recent article from Facebook, apps and websites that use their services send information "to make their content and ads better."[5]

"When you visit a site or app that uses our services, we receive information even if you're logged out or don't have a Facebook account," writes David Baser, Facebook Product Management Director. "This is because other apps and sites don't know who is using Facebook."

The promise of a better user experience does little to calm fears when you learn just how much personal information changes hands (even if you don't actively use these services). When you visit a website, the following information sharing might take place without your knowledge:

Browser		**Website**
Requests to the website's server	>	
Shares your IP address so the website knows where to send site content	>	
	>	Pulls browser and operating system information
	>	Grabs cookies, to see if you've visited before (to save logins or items in your cart, for example)
	<	Sends content back to your browser

	<	Requests browser to communicate with other companies providing content or services on the website
Website and app information to the third-party tools (like social media)	>>	

What specific information are these collecting and storing? A journalist from *The Guardian* downloaded the data profile of one user and found out.

Google

After downloading his data stored by Google, *The Guardian* writer Dylan Curran found his file included 5.5GB ("roughly 3 million Word documents") of information on his habits and personal life. Here are some of the things Google stores. [6]

Your location every time you turn on your phone, if you have location tracking turned on.

Search history, included deleted searches, across all your devices.

An advertisement profile based on your demographic information including: location, gender, age, hobbies, job, relationships, and income.

Other things they track:

- Every app and extension you use.
- YouTube watching history
- Every Google Ad I've ever viewed or clicked on

Other data: website bookmarks, emails, contacts, Google Drive files, photos, brands you've bought, calendar, Hangout sessions, music you listen to, Google Books you've purchased, phones you've owned, pages you've shared, steps you walk in a day.

Facebook

When he downloaded his Facebook data, Curran's measured 600MB (about 400,000 Word documents). Included in his information:

- Every Facebook **message, file, or audio message** you've sent or received
- Login locations, times, devices
- Guesses as to your interests, based on your likes and conversations
- Applications you've connected to your Facebook account
- They can access your webcam and microphone
- Photos, videos, music, search history, browsing history

Positive Perspective (Dr. Gokul Solai)

Just like any other tech innovation, you walk a tight a line between being menacing and beneficial. We need to understand the positives of all this shared data. The media gravitates toward negative, so that's what people remember.

For example, we have the ability to prevent terrorism or suicide, based on the Facebook posts shared by some of its users and the AI set up to flag these posts. They also can know if you were wearing purple on last December. Does that have a huge impact on your life? Versus being able to prevent a terrorist attack or save a life? We have to keep this balance in mind.

In the Workplace

According to a recent study, more than 40% of worldwide employers use artificial intelligence processes of some kind.[7] In many cases, these tools are implemented to increase work productivity and efficiency.

On-the-job surveillance at work is nothing new. Factory workers clock in and out of their shifts; IT departments can see website activity; agencies and law firms require hour-by-hour task disclosure. AI makes constant, pervasive surveillance worthwhile because every bit of data is potentially valuable and no extra burden on human workers.

New developments in AI-powered work surveillance include:

Amazon has invented a **wristband that tracks hand movements** of warehouse workers. It also uses vibrations to nudge them into being more efficient.

Software firm Workaday processes over 60 factors to **predict which employees will leave**.

Startup Humanyze makes **ID badges that track employees** around the office and reveal how well they interact with coworkers.

Slack messaging app helps managers **measure task completion** speed.

Companies pass out FitBits to **monitor physical activity** for insurance purposes and encourage active lifestyles.

Every year at steel processor SPS Companies, its 600 employees fill out a 30-minute confidential survey that asks if they feel supported by their managers and valued by the organization. For the most recent survey, they brought in AI to analyze responses instead of combing through surveys by hand.[7]

By assigning emotions and attitudes to the language used in open-ended questions, SPS is able to determine if staff feels optimistic, confused, angry, or overlooked. The results are tabulated and used to provide recommendations for department managers and the enterprise. In one example, SPS streamlined its healthcare plans after survey results showed employees were confused by their many options.

The amount of time saved by AI can revolutionize an organization. At a company that used a similar annual employee survey, six HR staffers spent three months to analyze 3,500 surveys. Managers would take another five months to create action plans based on the data. At SPS, HR has used time saved processing survey results to start new mental and physical health initiatives for employees.

There are many positive outcomes to these AI tech advancements ...

- Data from trackable badges can measure if the office layout helps or hinders collaboration
- Companies can see when workers are misbehaving or sleeping on the job
- AI can more effectively screen for red flags in expense reports
- Checks for safety gear and accidents can be more attentively made by AI
- Biases can be removed from the hiring process with complex resume-scanning algorithms
- Algorithms can highlight pay differences between genders and races

Yet, with all these benefits come potential vulnerabilities. The human element is sometimes needed to weigh pros and cons of a complicated, nuanced circumstance. Since most emotions are communicated non-verbally, technology that rely only on text-based data can miss the bigger picture. For example, an algorithm may flag an older employee for lower productivity but miss other positive contributions in more subjective areas like leadership, experience, or mentorship.

And as AI tools are used to make more hiring, firing, and pay decisions, psychological effects on anxious employees could cancel out any process improvements. In the case of SPS, employee surveys were confidential but not anonymous. Response analysis can include demographic data, answers on previous surveys, and other background information.

“I’m fully aware of a handful of people who didn’t want to take the survey because they had a fear of being tracked,” said Corey Kephart, SPS vice president of human resources.

In addition, some employment lawyers fear AI might contain biases that could lead to workplace discrimination. Employment and AI lawyer Garry Mathiason claims that any algorithmic bias is likely to have an outsize impact on minorities and other protected classes of employees. A hiring algorithm might notice a higher rate of sick days for people with disabilities and recommend against employing them.

Few laws govern what data can be collected at work and how it can be used. Many employees unknowingly consent to workplace surveillance when they sign their employment contract. The Equal Employment Opportunity Commission, the U.S. body that enforces workplace discrimination laws preventing workplace, hasn’t issued official rules for how AI can be used in human resources. However, in 2016 an agency panel concluded that the technology can potentially create new barriers for opportunities.

Positive Perspective (Dr. Gokul Solai)

When we focus only on the negative, we miss the mark on the purpose of these tools and why they were invented in the first place. When we do repetitive tasks our minds wander. Recent tech advancements help ensure task success by limiting mistakes. AI tools actually give employees back a level of self-accountably.

At some jobs, they measure productivity with a stopwatch and a checklist. Would you rather have a band on your wrist gently nudging you to refocus or a manager breathing over your every pause?

Companies have always wanted people to be at work, doing their jobs efficiently, and safe while they're there. These tasks were being done by management anyway, so why not do them better, with less effort and error? Companies benefit and, ultimately, so do human workers.

Medicine

According to a 2016 report from CB Insights, about 86% of healthcare provider organizations, life science companies, and technology vendors for healthcare are using artificial intelligence technology. By 2020, these organizations will spend an average of $54 million on artificial intelligence projects.[8]

Since the nature of medical diagnosis is so process-oriented and data-driven — collect symptom data, parse data, look for patterns, diagnosis, treat, measure effectiveness, repeat — artificial intelligence and machine learning is a powerful tool for doctors and drug makers.

With the increasing use of AI, powered by connected devices and systems, there are more potential openings for hackers to gain access to valuable personal information. Personal medical information in the marketplace is believed to be 10 times higher than credit card data, which makes data theft irresistible to cybercriminals.[9]

Healthcare-related data breaches have reportedly affected millions of people, including: identity theft, loss of benefits, asset theft, and personal data leaks. According to a recent survey, 36% of medical professionals said that they had experienced an incident related to cybersecurity in the current year.[9]

Aside from using AI to diagnose disease, recommend treatments, and develop new medications, a major benefit includes the open sharing of medical records throughout the industry. Data management is the most widely used application of artificial intelligence and digital automation. Robots collect, store, reformat, and trace data to provide faster, more consistent access.

"Insights gained from faster analysis of more data also helps patient education," explains Solai. "We can say 'This is what happened, and this is how you can help yourself with treatments and preventative measures.'"

Although transparency of medical records and data between institutions would create massive benefits, it is weighed against the security of that data.

“In the wrong hands, access to all this private data could lead negative consequences,” warns Solai. “Not only in identity theft, but if an insurance companies knows about a patient’s preexisting condition and then rejects them for coverage, for instance.”

Recently, an agreement to manage digital medical records between a UK machine learning firm and the Royal Free London NHS Foundation Trust was ruled unlawful by the government. The Information Commissioner's Office found the Royal Free failed to ask for patient consent before implementing and using AI technology. After the ruling and a damaging patient data leak, many healthcare technologists think the public will become "technophobic."[10]

Positive Perspective (Dr. Gokul Solai)

One of the amazing technologies to come out in this space is the use of smart watches by nurses. The watch is on them all the time, which means it doesn’t get misplaced. They are not intrusive, simple, and accessible.

Nurses are so overworked they don’t get time to spend with patients or make the best use of that time. Alerts, reminders, and patient data can be sent directly to them, improving communication, efficiency, and patient care.

Medicine is a field where “life-and-death impact” is literal, when it comes to AI and information access. These customizable supervisors help give better patient outcomes. Life-saving tech like this wouldn’t be possible without access to health data and the power of AI.[11]

(Read more in our whitepaper, “The iDoctor Will See You Now: Challenges and Implications Facing Future Healthcare AI”)

Human Rights

Though the previous areas of concern are only a few examples, the fundamental issue with AI's involvement with personal data is the same:

- What are people's rights, with regards to their personal information?
- How do we protect and enforce these rights?
- How do we enjoy the benefits of AI, while respecting those rights?

Often, the collection and creation of databases necessary for AI to work are used — with or without bad intentions — to make assumptions about people. Regardless of intent, many see these practices as an interruption of the fundamental rights to privacy and data protection.

"Many people assume that AI improves on human decision-making, associating computers with logic and imagining that algorithms automatically work against human biases or limitations," explains digital rights advocacy group, Access Now. "In fact, since human beings develop algorithms, they can and do replicate and reinforce our biases, and increasing use of AI may only work to institutionalize discrimination while diminishing human accountability for it."[12]

Even before AI became as sophisticated as it is today, researchers discovered bias in the algorithms used for university admissions, human resources, credit ratings, banking, the child support system, social security, and more. One example includes London's St. George's Hospital Medical in London in the 1980's. The school used an algorithm to comb through student applications and found it to discriminate against women and non-European-looking names.[13]

What's more, much of the use of artificial intelligence goes on without our explicit knowledge, in the backgrounds of our everyday interactions with the world.

Positive Perspective (Dr. Gokul Solai)

At some point, we will have to address these questions together. Laws and regulations can be beneficial, but only take us so far. While we used to expect a central, authoritarian power to hand down declarations, our society is breaking away from this mindset with the help of technology. Society will have to determine a united code and do so together.

The Moral Machine project at MIT is a small-scale example of this idea. They set up a social experiment to crowdsource the establishment of universal driverless vehicle ethics. Through a set of scenarios, people give input into how machines should process decisions. While not a perfect solution to the issue of human rights protection, we could learn a lot from this experiment.[14]

DATA

As we have seen with the previous examples (far from every threat that exists), if artificial intelligence technology is to overcome concerns from the public. Here are some steps technologists can take to protect data and trust of the consumer.

Data Encryption, Masking & Containerization

Encryption — converting information from a readable form to an encoded version that can only be decoded by a key — is seen by many as the first step in protecting personal data.

“Security is an endless race, and encryption, in short, protects people,” said Jane Horvath, senior director of global privacy at Apple.[15]

Differential privacy, for example, introduces randomness into aggregated data, reducing the risk of re-identification while preserving conclusions made from the data, explains Dr. Mark Wardle, a consultant neurologist and health informatics expert.

Homomorphic encryption, a more advanced technique, "allows information such as private medical data to be encrypted and subsequently processed without needing decryption," Wardle explained. "Such technology is, as far as I am aware, at a very early stage as it is extremely computationally-intensive."

Collected data can be also be masked or anonymized so that readers can't learn specific information about a specific user. Some companies use this approach with regulatory compliance, where "blind" enforcement policies use threat detection on devices without connecting identifying information. Apple's iOS 10 for mobile devices added similar privacy techniques. It can recognize app and data usage patterns among user groups while hiding the identities of individuals.

In the workplace, another best practice is containerization. By separating business and personal apps, enterprise mobility management tools analyze data from only corporate apps, while still preventing malware from infecting personal apps. Containerization allows IT departments to protect its organization without invading users' privacy on personal apps.

“Blockchain is another technology we can use to anonymize data, while keeping a trail for analysis,” says Solai. “We’re still learning how best to use this tech, but it could be beneficial for protecting invaluable personal information.”

Data Use Verification

AI research firm, DeepMind, is working to boost transparency and trust through a data access tracking process called Verifiable Data Audit (VDA).

"[VDA] is designed to allow partners to check on who has accessed data, when, and for what reason," says Andrew Eland, engineering lead for health at DeepMind. "It increases transparency by ensuring accurate 'spot checks' can be made on data access, creating real accountability."[10]

VDA differs from other audit systems by using cryptography to protect data from being changed without raising red flags.

"Whilst VDA will be useful for auditing access to health data, it could also be used to build trust in systems more generally," Eland says. "For example, creating unforgeable timestamps to make clear when something was written or created, or 'watermarking' data sets to ensure they have not been tampered with — something very important for the machine learning and academic communities."

The end goal of VDA is to allow patients, patient groups, and regulators to check their data is only being used for approved purposes.

Universal Regulations / Guidelines

A recent study showed that an average of 60% of consumers think their government should be doing more to increase data protection from AI.[16]

It's a challenge to dynamically regulate this space, but we should universally agree what we need to protect. Individual privacy security should be standardized throughout the world. Data is everywhere, it's circulating everywhere, so it has to be regulated everywhere.

"We don't want to prevent innovation, but we also have to recognize that we need to protect information. Especially personal information," Solai says.

Data privacy regulations differ from country to country. Whereas the European Union has the Data Protection Directive and forthcoming General Data Protection Regulation, the U.S. has no unifying standards. Instead, industry-specific laws govern the nation's data, individually. The Health Insurance Portability and Accountability Act (HIPAA) protects healthcare information. The Fair Debt Collection Practices Act limits creditors and financial institutions from sharing identifying information about a person's buying behaviors or debts.

But what should universal regulations include? At the most basic level, certain guidelines should be no-brainers.

- **Consent:** no data should be collected without an individual's knowledge and approval
- **Transparency:** a clear pathway to evaluate and understand collection purpose and uses
- **Protection:** robust digital security measures
- **Privacy by Design:** limit data collection to what is strictly necessary
- **Security by Design:** prevent data breaches, harmful interference, and exploitation
- **Accountability:** costly fines and sanctions for organizations who do not comply
- **Anonymity:** data should be disconnected from people's identities where possible

- **Bias-Proof:** algorithms used for sensitive purposes should be tested for bias and unintended consequences
- **Access:** individuals should be able to request and receive their own data

“As we try to develop universal regulations, we need to make it a priority to provide a voice to all people,” adds Solai. “Since universal guidelines protect everyone, there’s a social responsibility to not lean only on a centralized body to dictate laws. Social decisions with this much weight should align with as many people as possible.”

EU's General Data Protection Regulation (GDPR)

Some see the European Union's GDPR as a good framework, or test case, to expanded global data governance. Starting on May 28, 2018, the new regulation's goal is to give people more control over, and assure greater security for, their personal data.

Complex algorithms used in AI can draw conclusions about individuals with sometimes unwelcome (even unintended) effects — including biasing, profiling, and discrimination — as we have seen in the "Sources of Threat" section. The GDPR aims to prevent these negative actions through increased transparency and accountability.

Highlights of the regulation include:

- A “right to explanation,” so users are informed about the logic of decision-making algorithms
- The requirement for these logic explanations to be simple enough for people to understand
- The right for users not to be illegally profiled by automated processing
- Consent to AI processing must be given freely, specific, “unambiguous,” and a “clear affirmative action” like selecting a checkbox on a website

While there are many challenges for EU businesses to comply to GDPR — the ability to explain complex algorithms in human terms, for one — many believe it to be a first step toward an eventual resolution to data privacy concerns. Businesses who do not comply face heavy fines and consequences, which itself gives assurance to the public of the priority given to protecting personal information.

Use AI to Combat Data Fraud

“AI’s higher processing power makes it the ideal digital gatekeeper,” says Solai.

It's common sense, if you think about it. But who better to monitor tons of data for abnormal use patterns and risky behavior than artificial intelligence itself? IT researchers already use algorithms to learn and predict new malware. Al-based, self-learning security systems hold the promise of automatic cyber defense in the future.

"Privacy-preserving machine learning offers an interesting technological approach to addressing questions about data access and governance," says Peter Donnelly, Chair of the Royal Society Machine Learning Working Group.

One method has tying people's unique behavioral characteristics to their traditional demographic and biometric information. Any change in behavior can signal a possible fraud threat for further investigation. The challenge to make this technique a reality has always been scrutinizing the masses of data from each person and point. Fortunately, that's the biggest strength of machine learning, RPA, and AI.

One new example? Software firm Onfido has developed a Facial Check with Video authentication that asks users film themselves performing randomized movements. Using machine-learning, the video is evaluated against a user's identity profile.

"Artificial intelligence and machine learning are crucial security capabilities to interpret the complexity and scale of data available in today's digitally connected world," explained Johan Gerber, EVP of security and decision products at Mastercard. The credit card company uses AI to authenticate payments.

Not only can AI be used to combat fraud in the moment, but its pattern recognition capability makes it ideal for prevention. When cybercriminals act, they leave behind evidence.

"When collected and studied by machines, these can provide tremendous insight into the tools, resources and motivations that these modern criminals have," said Greg Day, vice president and chief security officer at Palo Alto Networks. "Access to rich threat intelligence data and the ability to 'learn' from that data will ultimately empower organizations to stay one step ahead of cybercrime."[3]

Use Humans as Gatekeepers

How much influence we should give machines could be based on how much decisions effect people's lives. For sensitive decisions that require complex, nuanced reasoning, empathy, and wise judgement, humans are still a better choice.

"Shopping recommendations generated by algorithms? No big deal," says Eduardo Ustaran, co-director of the global Privacy and Cybersecurity practice of Hogan Lovells. "Being eligible for a certain school, a career-defining promotion, or life-saving medical treatment? Get a human involved pronto." [17]

As Microsoft's Dr. Hsiao-Wuen Hon claims, computers are "the best-ever left brain" (logic and rationality) and humans have "the best-ever right brain" (creativity, judgment, wisdom). [18] Using robots to process data and humans as an approver or final check takes advantage of both strengths.

“We have to use a subjective source of reasoning for some decisions,” says Solai. “Historically, robotics has been bound by Asimov’s three rules; however, these rules could never replace human thought or relating to people.”

“AI can be the gatekeeper for certain things, but human validation is still important.”

CONCLUSION

But First … Educate, Earn Trust, Gain Consent

"[Personal] data is terrifically valuable, powerful, and offers tremendous scope to do good," says neurologist and health informatics expert Dr. Mark Wardle. "But we also have a great responsibility to protect that data and ensure access is safe, secure, and transparent,"[18]

The biggest barrier to a future partnership between humans and AI may not be lack of laws, need for protections, or data masking requirements. Without societal trust and consent to use AI tools, these steps would be pointless.

Data protection awareness and consumer education will become key to for AI firms to earn confidence in their solutions. Organizations will need specific internal governance guidelines for AI, not only for technical and data input processes, but also addressing legal and ethical issues. An added bonus to enforced internal regulations is the feeling of security it gives consumers.

"If a [consumer] can understand what's being proposed, can see the benefits, and can make the balance for themselves of the risk to their privacy versus the benefit to their [life], I think you'll find they'll be more compelled to participate in [beneficial AI tech]," said Nathan Lea, senior research associate at UCL's Institute of Health Informatics and the Farr Institute of Health Informatics Research.

Creating societal trust starts with the organizations using automation, adds Solai. He recommends companies follow these techniques to build a culture of trust.

Manage expectations:
"Not everyone will immediately embrace disruptive tech like AI. And that's OK."

Be open to people's right to choose:
"Don't hide opt-out information or privacy policies."

Start with optimism:
"The AI implementation process will have challenges, which might include its adoption. But overcoming them will make solutions better."

Embrace human resilience to innovation:
"Look back at where we've come from. In the stone age, we were probably afraid of fire. If we let that stop us, we wouldn't have the combustion engine. And the modern economic growth in manufacturing came from automated robots that people were scared would replace them."

Avoid over-reliance on AI:
"Partnering RPA with strong leadership, data integration and analytics, and business process management is the true path to digital business innovation."
(See "The iDoctor Will See You Now," Novatio Whitepaper)

Choose the Right AI Partner:
When selecting the right digital workforce products, you need a flexible, knowledgeable leader — especially one well-versed in both understanding the concerns of data privacy protection and benefits of artificial intelligence technology. Trust a partner who can give experience-based guidance on how to accommodate for digital workforce implementation and transformational leadership.

For 25 years, Novatio Solutions has provided this leadership in managed business process (BPO) outsourcing for Fortune 100 clients. They have returned more than 500,000 hours back to their partners, so that those organizations' employees can focus on higher-value work. They have helped free managers from micromanaging. And they have helped empower people to harness the cognitive skills that make them human.

"The Novatio team understands automation and what it takes to transform business operations," says Dr. Gokul Solai, head of products and alliances for Novatio. "Our goal is to use digital workforce solutions to make everyone's life easier, from the CEO to the person answering the phones."

It's this top-to-bottom understanding of human workers and end users—their natures, fears, desires, and needs—that allows that allows for successful system transitions and solution adoptions. Novatio Solutions provides a versatility of implementations for a wide variety of companies in fields such as tech, finance, government, transportation, insurance, healthcare, retail, and manufacturing.

Novatio Digital Workforce

- Noninvasive, technology-agnostic workforce
- 100% compliance
- Zero errors
- 3-5 times greater productivity
- 1/10 price of traditional workforces
- 2-3 times faster implementation than other solutions

Humanistic Mindset
When evaluating AI technology solutions, the "what" and "why" — helping people live better, longer, more healthy lives —should be prioritized over the how.

"The most efficient solution might be what you want from technology," says Solai, "But is it the safest most helpful solution?"

Their focus on the people impacted by the technology, instead of the technology separates Novatio from other firms.

SOURCES

1 "AI-Spy: The Workplace of The Future," The Economist, https://www.economist.com/news/leaders/21739658-artificial-intelligence-pushes-beyond-tech-industry-work-could-become-faireror-more, March 28, 2018

2 "Artificial Intelligence Data Privacy Issues on The Rise," https://searchmobilecomputing.techtarget.com/news/450419686/Artificial-intelligence-data-privacy-issues-on-the-rise

3 "The Role of AI and Machine Learning in Personal Data Security," Raconteur, https://www.raconteur.net/technology/the-role-of-ai-and-machine-learning-in-personal-data-security

4 "Report: 71% Of Consumers Fear AI Will Infringe on Their Privacy," TechRepublic, https://www.techrepublic.com/article/report-71-of-consumers-fear-ai-will-infringe-on-their-privacy/

5 "Hard Questions: What Data Does Facebook Collect When I'm Not Using Facebook, and Why?" Facebook Newsroom, https://newsroom.fb.com/news/2018/04/data-off-facebook, David Baser, Product Management Director

6 "Are You Ready? This Is All The Data Facebook And Google Have On You," The Guardian, https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy, Dylan Curran

7 "What's on Your Mind? Bosses Are Using Artificial Intelligence to Find Out ," The Wall Street Journal, https://www.wsj.com/articles/whats-on-your-mind-bosses-are-using-artificial-intelligence-to-find-out-1522251302, Imani Moise, March 28, 2018

8 "The iDoctor Will See You Now: Challenges and Implications Facing Future Healthcare AI," Novatio Solutions, http://novatiosolutions.com/wp-content/uploads/2017/09/novatio_white_paper_v5.pdf, August 2017

9 "How important is Data Security in the Age of Artificial Intelligence?" Entrepreneur, https://www.entrepreneur.com/article/306623, Ashim Roy

10 "AI Has No Place in The NHS If Patient Privacy Isn't Assured," WIRED UK, http://www.wired.co.uk/article/ai-healthcare-gp-deepmind-privacy-problems, Nicole Kobie

11 Mobile Village, "RistCall Patient Care App Puts Patient Alerts on Smart Watches," http://www.mobilevillage.com/harbinger-ristcall-patient-care-app/

12 "Artificial Intelligence: what are the issues for digital rights?" Access Now, https://www.accessnow.org/artificial-intelligence-issues-digital-rights/

13 "The Problem With Algorithms: Magnifying Misbehavior," The Guardian, https://www.theguardian.com/news/datablog/2013/aug/14/problem-with-algorithms-magnifying-misbehaviour

14 "Driverless Cars and MIT's Test of the Crowdsourcing Morality," Financial Times, https://www.ft.com/content/8fc7fde0-7f21-11e6-8e50-8ec15fb462f4, Anjana Ahuja, Sept. 20, 2016

15 "Artificial Intelligence Poses Data Privacy Challenges," Bloomberg Law, https://www.bna.com/artificial-intelligence-poses-n57982079158/, Stephen Gardner

16 "The Consumer: Sees AI Benefits But Still Prefers The Human Touch," Genpact, http://www.genpact.com/downloadable-content/the-consumer-sees-ai-benefits-but-still-prefers-the-human-touch.pdf)

17 "Is Artificial Intelligence the Ultimate Test for Privacy?" HL Chronicle of Data Protection, https://www.hldataprotection.com/2018/03/articles/consumer-privacy/is-artificial-intelligence-the-ultimate-test-for-privacy/

18 "Artificial intelligence (AI) + Human intelligence (HI) = (collective) intelligence (amplified) or super intelligence," LinkedIn, https://www.linkedin.com/pulse/artificial-intelligence-ai-human-hi-collective-super-nekaj-%E5%AE%87-%E8%B5%AB, Epi Ludvik Nekaj, Feb. 23, 2017

ABOUT NOVATIO SOLUTIONS

Novatio Solutions is a Digital Workforce provider from the founders of Solai & Cameron Technologies. The company capitalizes on Solai & Cameron's 25 years of experience developing best practices in operational transformation.

Novatio harmonizes multiple robotic process automation (RPA) tools along with next generation technology to create a customized digital workforce. Consequently, Novatio's clients benefit from added capacity, scalability, and efficiency.

“Traditional” automation solutions usually fall short in their rigidity. They are limited in scope and benefits and too expensive to update or change. There’s a long change process that is highly disruptive to teams and systems. And, they require more internal technical resources.

In many cases, companies rely on legacy applications or systems that are no longer supported. When changes or integrations are needed, technical support resources are difficult to find. Novatio Solutions harmonizes multiple and previously disconnected robotic process automation (RPA) tools and combines them with next-generation technology to create a customized digital workforce. Robotic process automation with digital workers gives agility and flexibility to accommodate change; decreases time to value; and is less expensive to set up and maintain.

The Novatio online portal offers advanced business intelligence tools, an online marketplace and service catalog and visibility into usage and billing. Simulator tools provide real-time input on cost-savings, which prioritizes time and cost efficiency. The portal also provides insight into forecasting and demand prediction, which allow for to data-driven staffing and a more proactive decision-making.

For more information, visit NovatioSolutions.com.