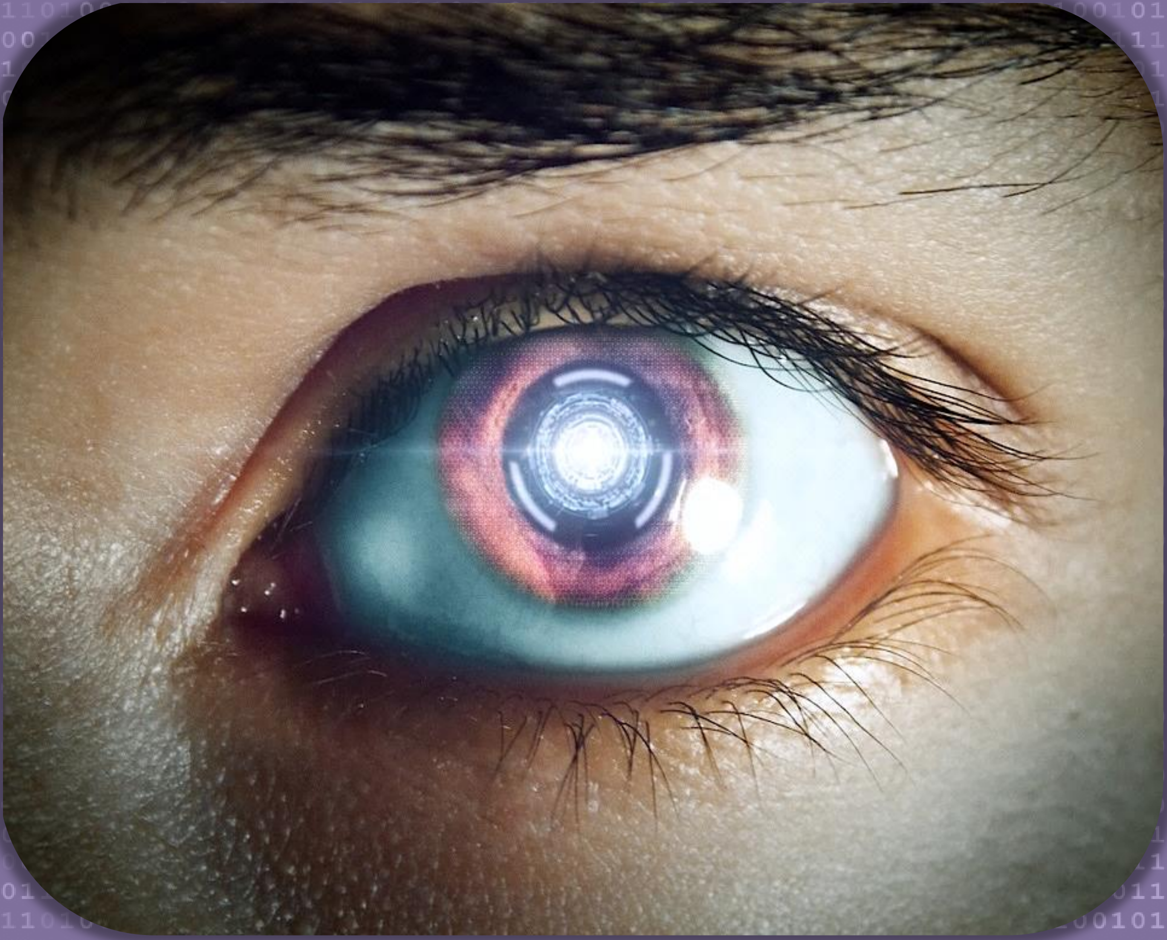


THERE'S NOWHERE TO HIDE

Artificial Intelligence and Privacy in the Fourth Industrial Revolution

Lead Authors: Sarah W. Denton and Eleonore Pauwels

Supporting Authors: Yujia He and Walter G. Johnson

Policy Report | March 2018

WILSON CENTER 50 years

synenergene
Responsible Research and Innovation in Synthetic Biology

i3p
Institute for
Philosophy &
Public Policy

At its core, artificial intelligence (AI) optimizes data. Machine-learning algorithms, one component of AI, are trained using massive datasets curated by humans to predict various aspects of our daily lives. Such predictive intelligence could be a positive force amplified by continued decentralization of the technology. Or, ubiquitous cognition and surveillance could be a disruptive force amplified by the unregulated proliferation of AI technologies. Yet, though we will certainly see more and more AI systems being integrated into every facet of our infrastructures, homes, and bodies, the proliferation of AI technology isn't the problem. A privacy-security quagmire arises from the interconnectivity of AI systems that optimize every aspect of our lives including our genomes, faces, finances, emotions, and environments. We will no longer be able to hide from the ubiquitous sensory capabilities built into our infrastructure. The convergence of AI, the Internet of Things (IoT), and the related Internet of Living Things (IoLT) will operate in the background of our lives – constantly refreshing. Omnipresent and omniscient data capture and optimization pose threats to our privacy and security. As a society, our ability is limited to anticipate and mitigate the risks that AI and IoT technologies are creating for our privacy and collective security.

In the future, your identity – the entire history of you – exists within a vast array of interconnected databases of faces, genomes, emotions, and thoughts. Your personal algorithmic avatar, the digital representation of your most intimate data streamed to the cloud, might be the next target for hackers, governments, and private companies. Just imagine…

> *It's 6am and your AI personal assistant Niko greets you. As you walk into the bathroom, Niko connects to your smart mirror to analyze your saliva and biometric data, cross-referencing it with your face image database to identify subtle changes in your health. Your life-cycle user platform is reflected around your face, – height 5'11", weight 157lbs, blood pressure 139/99, nutrition levels, genetic variations – quantifying your health in real-time via the Aegis implant in your arm. Streamed to the cloud, these biological data track your health, connect with physicians, and build powerful collective datasets for precision medicine.*
>
> *In an instant, the Aegis profile disappears, leaving your reflection seemingly bare. Then, Niko reminds you that your driverless car is arriving in 30 minutes. Your location is a core data point, which the Aegis constantly updates, sending data to the cloud every five minutes.*
>
> *En route to the office, you notice the cameras equipped with facial and biometrics recognition software installed in each streetlight. They are part of the new City Brain, a comprehensive cognitive network that records and rates everyone's behaviors and interactions. Your smart car pulls up to the front doors of your office building and your Aegis unlocks the elevator. Your mind drifts back to the smart streetlights: "I wonder if they know I went to that DIYbio meeting last night." Days later Niko notifies you, "I've put a reminder in your calendar – you are scheduled to appear in court regarding your attendance at an outlaw meeting."*

While this scenario is still hypothetical, the potential privacy and security quagmire is not – and these technologies (though in their infancy) are emerging at an increasing rate.

Although artificial intelligence (AI) does not have a standard definition, it generally refers to "the use of digital technology to create systems that are capable of performing tasks commonly thought to require intelligence. Machine learning is variously characterized as either a sub-field of AI or a separate field, and refers to the development of digital systems that improve their performance on a given task over time through experience."[i]

Using computational algorithms enhanced with machine-learning capabilities, AI is able to analyze and optimize sensory data (i.e., images of your face, recordings of your voice, your vitals, and even your DNA) faster and better than humans. Despite the numerous questions surrounding AI, companies and governments around the world are forging ahead in developing these technologies. Even if global AI innovation doesn't ensure proliferation, it does enable us to imagine it. So – what if it *actually* happens?

The world around us would be equipped with sophisticated sensory capacities. We could identify the genetic composition of our bodily fluids, help catch killers, and selectively enhance our memories[ii]. Portable genomic sequencers in our smartphones the size of a USB stick would become part of our interconnected sensory networks—what we already call the Internet of things (IoT). If millions of people streamed their personal data to the cloud, they would build the most powerful health dataset the world has ever seen. When the genetic and neural identity of a living thing resides in the cloud, a new form of life is created on the Internet – enter the age of the Internet of Living Things (IoLT). In the future, our neural data – our thoughts, feelings, and memories – might be monitored via brain-computer interfaces (BCIs) implanted in our skulls. If this becomes reality, our minds and bodies will no longer exist solely within the physical world.

At its core, artificial intelligence (AI) optimizes data. Machine-learning algorithms, one component of AI, are trained using massive datasets curated by humans to predict various aspects of our daily lives. Such predictive intelligence could be a positive force amplified by continued decentralization of the technology. Or, ubiquitous cognition and surveillance could be a disruptive force amplified by the unregulated proliferation of AI technologies. Yet, though we will certainly see more and more AI systems being integrated into every facet of our infrastructures, homes, and bodies, the proliferation of AI technology isn't the problem. A privacy-security quagmire arises from the interconnectivity of AI systems that optimize every aspect of our lives including our genomes, faces, finances, emotions, and environments. We will no longer be able to hide from the ubiquitous sensory capabilities built into our infrastructure. The convergence of AI, the Internet of Things (IoT), and the related Internet of Living Things (IoLT) will operate in the background of our lives – constantly refreshing. Omnipresent and omniscient data capture and optimization pose threats to our privacy and security. As a society, our ability is limited to anticipate and mitigate the risks that AI and IoT technologies are creating for our privacy and collective security.

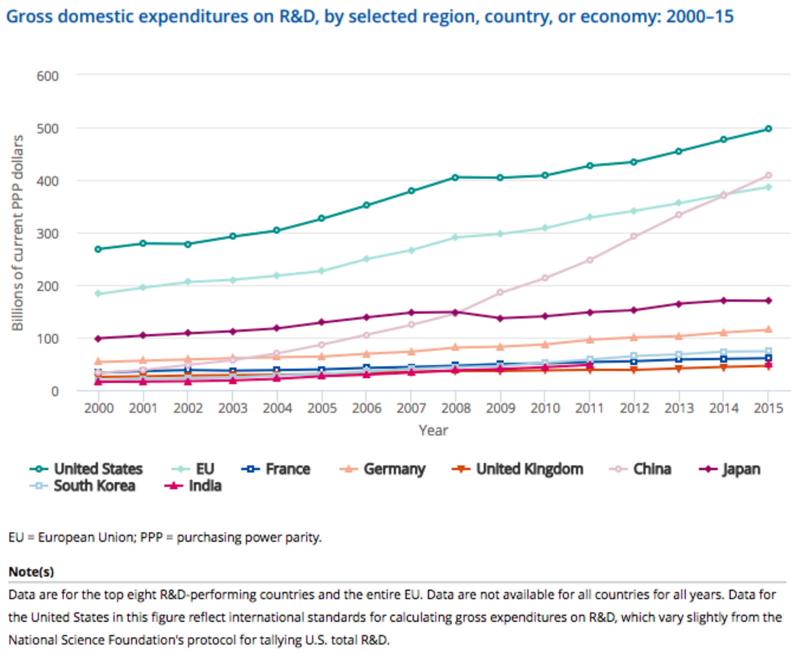
In the most general sense, privacy can be thought of as our right to selectively reveal our selves. Information such as our medical records, finances, photos, and a wide range of other data are considered private unless the individual explicitly chooses otherwise. According to the United Nations (UN) General Assembly resolution 68/167:

> “The human right to privacy, [affirms that] no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, and recognize[s] that the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interferences, and is one of the foundations of a democratic society.”

Unfortunately, the road to global predictive intelligence is littered with challenges to the protection of privacy. Governments and companies alike will reap significant benefits from the proliferation of AI-enhanced IoT and IoLT devices. For instance, Oxford Nanopore Technologies’ portable genome sequencer MinION and Metrichor, an intelligent bio-lab of the future[iii], are just two examples AI in epidemiology (i.e., the population-level comprehensive science that describes the risk of disease in quantitative and qualitative terms[iv]). Another example is Sequenom Inc., which translates genetic code into relevant insights and has applied for a United States patent on a non-invasive assessment of genetic variation.[v] AI epidemiology could allow governments to easily monitor the spread of disease and prevent epidemics. But AI epidemiology isn’t the only application of AI that could benefit governments. Skydio’s new biometric tracking drone could provide law enforcement with better tracking capabilities than ever before. And connecting our brains to the Internet with BCIs could pave the way for applications such as a collective cloudmind – where “multiple individual minds (human or machine) merge to pursue collaborative goals such as problem solving, idea generation, creative expression, or entertainment.” What if the cloudmind became mandated by the state under the guise of national security? The right to privacy does not exist only insofar as the state deems necessary to protect the security of the collective.

Moving Towards Global Predictive Intelligence

We are currently living in the Fourth Industrial Revolution, an age that builds upon the digital revolution with a global surge in big data capacities and uses. This new industrial era seeks to merge the physical and the digital, and laboratories are no exception. Technological advances in genomics, synthetic biology, AI, automation, and cloud computing – all hallmarks of the Fourth Industrial Revolution – are increasingly converging and enabling each other. [vi] The convergence of AI, biology, and neuroscience will usher in a new wave of AI characterized by the proliferation of devices capable of analyzing cellular, genomic, and even our neural data, affecting almost every major industry.


Gross domestic expenditures on R&D, by selected region, country, or economy: 2000–15

EU = European Union; PPP = purchasing power parity.

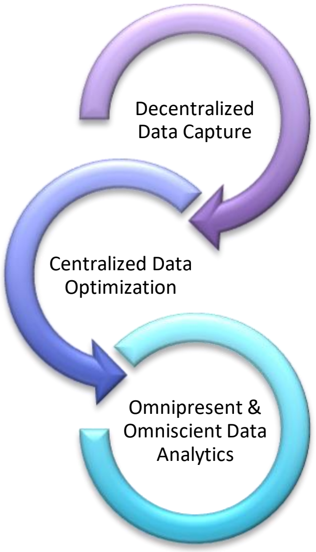
Note(s)

Data are for the top eight R&D-performing countries and the entire EU. Data are not available for all countries for all years. Data for the United States in this figure reflect international standards for calculating gross expenditures on R&D, which vary slightly from the National Science Foundation's protocol for tallying U.S. total R&D.

The light pink line shows China’s sharp increase in R&D spending.
Image: National Science Foundation

China and the United States (US) are leading in the development and application of AI technologies, and other countries such as India are trying to catch up. [vii] The National Science Foundation recently released comprehensive data showing that China is steadily rising to meet US research and development spending. "China's spending on R&D grew by an average of 18% per year between 2010 and 2015 – more than four times faster than US spending."[viii] China's ambitious, but more relaxed, AI policy and enormous datasets collected on its citizens gives China an advantage in AI training.[ix] The US on the other hand, does not have a national AI policy; in 2016, the Obama administration published two reports: one by a subcommittee of the National Science and Technology Council and one focused on an R&D strategy. India is also increasing its AI spending; the AI sector grew 100% in H1 2017 in comparison to H2 2016 and is poised to grow to $16.06 billion by 2022.[x] With such global increases in R&D spending with no signs of slowing down, it's more important than ever for ethicists and policymakers to consider the implications of these emerging technologies.

Data fuels the AI economy and will become intertwined with the very body parts, qualities, artifacts and quirks that make us human. Our cells, genomes, thoughts, and emotions will be transformed into individual pieces of data that could dictate health insurance rates, likelihood that a crime will be committed, and predict epileptic episodes. However, the spread of AI innovation across the globe isn't the whole of the problem. It lies deeper in the pervasive optimization of our most intimate data. When AI converges with IoT and IoLT devices our faces, voices, genomes, and neural data may become centralized, giving companies and governments unprecedented insight into the population – often without informed consent and adequate data security mechanisms. Data capture and optimization does not only potentially threaten our privacy, both processes are also vulnerable to cyberattacks conducted by governments and non-state actors alike. But, how do companies and governments acquire our personal data? Are citizens knowledgeable and aware of the data generated on their daily interactions? How will notions of privacy fare in the face of comprehensive cognition and predictive intelligence? Does it matter?


Decentralized Data Capture
Centralized Data Optimization
Omnipresent & Omniscient Data Analytics

Omnipresent & Omniscient Data Analytics

In this global predictive intelligence revolution, omnipresent and omniscient data optimization will transform our lives. AI, as a set of pervasive technologies with inherent dual-use implications, could be used to promote equity, justice, and compassion. Alternatively, it could be used to oppress, deceive, and manipulate populations. Imagine you live in a smart city, where everything from your banking information and healthcare records to your DNA and biometrics data are interconnected in the City Brain – where can you hide?

Smart Cities & IoT

According to IBM, "Smart Cities are designed to utilize information and telecommunications methods to sense, analyze and integrate various pieces of key information from core systems used in city operations, and to respond intelligently to a variety of needs relating to the environment, public security, city services, commercial activities and citizens' livelihoods."

Smart cities share at least three common characteristics: 1) broad, continuous data collection from sensors, cameras, or other devices; 2) seamless access to data from many connected data collection systems; and, 3) infrastructure and tools to store and analyze large amounts of data.[xi] The infographic below shows the multitude of ways AI may be integrated into cities around the globe.

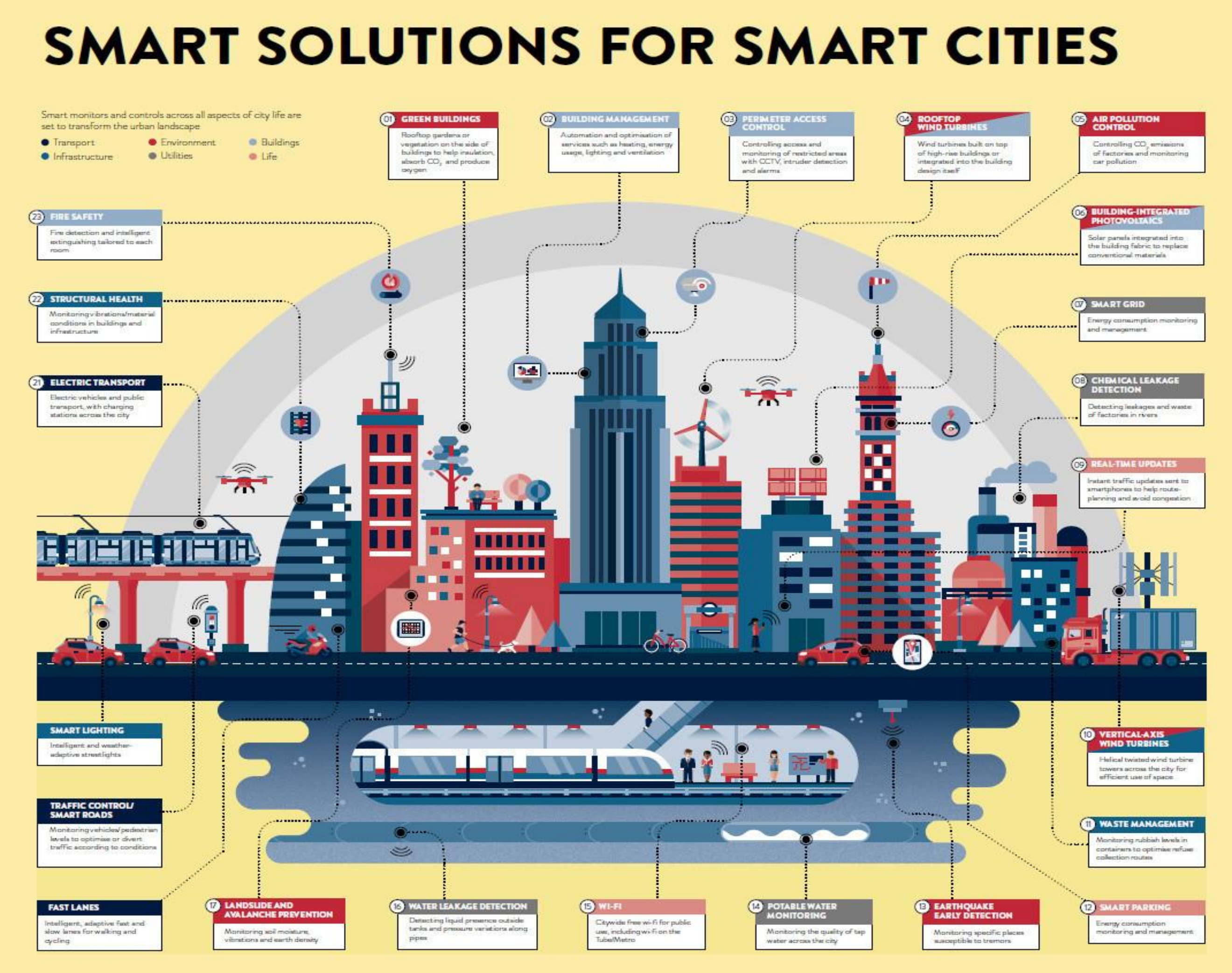

SMART SOLUTIONS FOR SMART CITIES
Smart monitors and controls across all aspects of city life are set to transform the urban landscape
● Transport
● Infrastructure
● Environment
● Utilities
● Buildings
● Life
01 GREEN BUILDINGS
Rooftop gardens or vegetation on the side of buildings to help insulation, absorb CO2 and produce oxygen
02 BUILDING MANAGEMENT
Automation and optimisation of services such as heating, energy usage, lighting and ventilation
03 PERIMETER ACCESS CONTROL
Controlling access and monitoring of restricted areas with CCTV, intruder detection and alarms
04 ROOFTOP WIND TURBINES
Wind turbines built on top of high-rise buildings or integrated into the building design itself
05 AIR POLLUTION CONTROL
Controlling CO2 emissions of factories and monitoring car pollution
06 BUILDING-INTEGRATED PHOTOVOLTAICS
Solar panels integrated into the building fabric to replace conventional materials
07 SMART GRID
Energy consumption monitoring and management
08 CHEMICAL LEAKAGE DETECTION
Detecting leakages and waste of factories in rivers
09 REAL-TIME UPDATES
Instant traffic updates sent to smartphones to help route-planning and avoid congestion
10 VERTICAL-AXIS WIND TURBINES
Helical twisted wind turbine towers across the city for efficient use of space
11 WASTE MANAGEMENT
Monitoring rubbish levels in containers to optimise refuse collection routes
12 SMART PARKING
Energy consumption monitoring and management
13 EARTHQUAKE EARLY DETECTION
Monitoring specific places susceptible to tremors
14 POTABLE WATER MONITORING
Monitoring the quality of tap water across the city
15 WI-FI
Citywide free wi-fi for public use, including wi-fi on the Tube/Metro
16 WATER LEAKAGE DETECTION
Detecting liquid presence outside tanks and pressure variations along pipes
17 LANDSLIDE AND AVALANCHE PREVENTION
Monitoring soil moisture, vibrations and earth density
FAST LANES
Intelligent, adaptive fast and slow lanes for walking and cycling
TRAFFIC CONTROL/ SMART ROADS
Monitoring vehicles/pedestrian levels to optimise or divert traffic according to conditions
SMART LIGHTING
Intelligent and weather-adaptive streetlights
21 ELECTRIC TRANSPORT
Electric vehicles and public transport, with charging stations across the city
22 STRUCTURAL HEALTH
Monitoring vibrations/material conditions in buildings and infrastructure
23 FIRE SAFETY
Fire detection and intelligent extinguishing tailored to each room

Image: Visual Capitalist

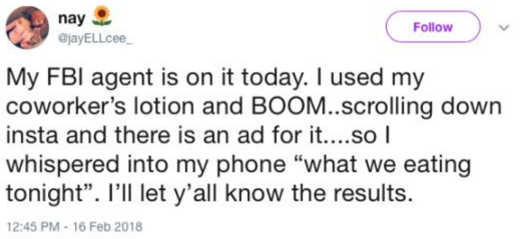
Currently, China is leading the way in smart city technology innovation and implementation. Tech giant Alibaba has been collecting massive amounts of data on citizens for its City Brain project, which was recently implemented in Malaysia.[xii] Alibaba's Apsara computing engine powers the City Brain, which is intended to solve a range of socio-political problems from traffic congestion, emergency dispatch, and crime prevention. According to Hua Xiansheng, a machine vision scientist at Ali Cloud, "City Brain is an unprecedented…experiment of bringing artificial intelligence into city planning." More than 500 cities in China have started, or are expected to start, evolving into smart cities. By the end of March 2017, 95% of provincial capitals and 83% of large cities were in transition to smart cities[xiii], which outpaces the US in smart city development. In the US, the New Orleans Office of Performance and Accountability used AI software to produce a map that shows the city blocks where fire deaths were more likely to occur and where the Fire Department could target its smoke-detector distribution program.[xiv] Programs like the

Smart America Challenge have inspired public-private smart city partnerships in major cities like San Jose, Boston, Chicago, Columbus, and New York City.[xv]

Within smart cities, marketing, transportation, healthcare, and law enforcement industries are increasingly implementing data optimization technologies. Below are examples from just a few of the primary industries poised to be majorly impacted by the convergence of AI, IoT, and IoLT technologies.

Advertising & Propaganda

Facebook, Google, and Alibaba are prime examples of how data monopolies can generate data on its users to target and personalize advertisements. Recently, Facebook has been under scrutiny for its connection to Cambridge Analytica, which markets itself as "providing consumer research, targeted advertising and other data-related services to both political and corporate clients."[xvi] This sort of precise, targeted advertising is a potentially valuable state propaganda tool; even though companies benignly use it to sell you their wares. Have you ever logged onto Facebook for a momentary break from reality only to be bombarded with advertisements for something you recently searched for on Google or Amazon? You're not alone. Anyone who interacts with the Internet on a regular basis can empathize with the FBI agent meme's poignancy. Our notions of privacy are already changing in response to the proliferation of technology. The idea of precise, targeted, personal surveillance is now a meme, something to be joked about; but it's something that governments and police forces around the world are quickly taking advantage of.



nay 🌻
@jayELLcee_

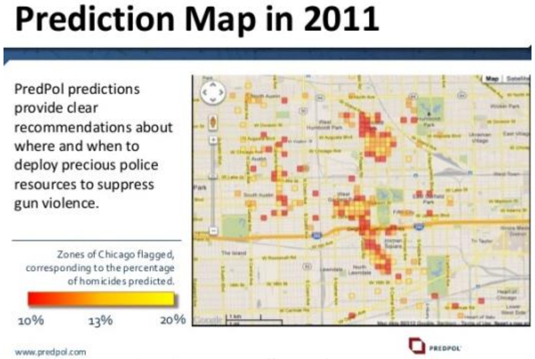
My FBI agent is on it today. I used my coworker's lotion and BOOM..scrolling down insta and there is an ad for it....so I whispered into my phone "what we eating tonight". I'll let y'all know the results.

12:45 PM - 16 Feb 2018

For example, the United Kingdon (UK) Home Office and ASI Data Science developed a tool using advances in natural language analyses and image recognition to identify Islamic State of Iraq and Syria (ISIS) (also known as Daesh) propaganda videos published online.[xvii] According to ASI Data Science, the software is not platform-specific and can be configured to detect 94% of ISIS video uploads; "anything the software identifies as potential ISIS material would be flagged up for a human decision to be taken."[xviii] Home Secretary Amber Rudd says, "The purpose of these videos is to incite violence in our communities, recruit people to their cause, and attempt to spread fear in our society. We know that automatic technology like this can heavily disrupt the terrorists' actions, as well as prevent people from ever being exposed to these horrific images." But there are still questions remaining as to the accuracy of such tools. How was the AI trained to identify specifically ISIS terrorist videos? Could it be biased? Could it be retooled and used to target vulnerable groups for harm or oppression?

Law Enforcement

In law enforcement and security contexts, predictive policing refers to, "the application of analytical techniques – particularly quantitative techniques – to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions."[xix]



Prediction Map in 2011

PredPol predictions provide clear recommendations about where and when to deploy precious police resources to suppress gun violence.

Zones of Chicago flagged, corresponding to the percentage of homicides predicted.

Image: Predpol (2015) "Predictive Policing on Gun Violence Using Open Data"

In the US, PredPol aims to reduce "victimization and keep communities safe," providing law enforcement agencies with customized crime predictions software that analyzes crime type, location, and date/time. To achieve this goal, predictive policing software like PredPol will have to overcome its reliance on historical data and invest in more real-time data collection and analysis. Even more disturbing, it is estimated that half of Americans are in the Federal Bureau of Investigation's (FBI) unregulated face recognition database, the Next Generation Identification Interstate Photo System (NGI-IPS). [xx] According to Georgetown University's *Perpetual Line-Up*, a May 2016 Government Accountability Office (GAO) report found that "the FBI had failed to issue mandatory privacy notices required by federal law, failed to conduct adequate accuracy of the FBI face recognition database (NGI-IPS) and the state databases that the FBI face recognition unit accessed, and failed to audit the state searches of the FBI face recognition database or any of the face recognition unit's searches."[xxi]

Uncanny Vision, a Bengaluru-based AI surveillance technology company, uses deep learning vision algorithms to enable real-time actionable surveillance and analytics.[xxii] According to Uncanny Vision's website, "[the] major differentiator with the award-winning Uncanny Surveillance software is to run artificial intelligence (deep neural networks) algorithms fully on a smart camera and interpret video as information before sending it to the cloud." China is also implementing more closed-loop systems like Uncanny Vision that perform data analytics on the device before sending it to the cloud. Chinese police forces are already implementing these AI-augmented glasses to sift through individuals easily in real-time at train stations and airports.

GLXSS ME smart glasses AI version

The first time, the first point of view, 33.4 grams of smart glasses, millisecond detection - to identify the target. To simulate the visual perception of the human eye,
Real-time, personal connection data; online perception, human-computer integration.

英特尔Movidius® Myriad视觉处理器
为AI芯片定制的神经网络推理框架
0.4克光学模组，大师级人机工学
适配主流手机与专业终端
于工业、制造、通信业、安防警务
与医疗领域商业化落地

Image: LLVision GLXSS Me Smart Glasses

Yet, machine-learning vision algorithms aren't the only kind of AI-based surveillance technologies. India has mandated citizens to enroll in Aadhaar, which identifies individuals based on their demographic and biometric information. According to the Unique Identification Authority of India (UIDAI) website, "[Aadhaar] is a scalable ecosystem for the purpose of instant authentication of residents…achieved through the process of demographic and biometric duplication, which compares information collected during the enrollment process with records in the UIDAI database." India recently released a revised draft of the DNA Fingerprinting bill originally proposed in 2015. The bill has been widely criticized for its privacy over-reach and the creation of two new institutions: the DNA profiling board and the DNA databank.[xxiii]

Healthcare and Smart Hospitals

Data monopolies like Google, Apple, and 23andMe are capitalizing on AI healthcare, using patient data to train their algorithms for a variety of applications, clinical and otherwise. Internet of Things (IoT) devices such as Fitbits synchronize smartphones to enable users to capture their movements and heart rate.[xxiv] Apple takes individual-level data collection a step further with ResearchKit, enabling researchers to solicit patients for large sale studies based on patient-reported data. Modern means of data collection are creating new data formats, and these new domains are bolstering clinical trial data collected by traditional means with considerable reliability[xxv].

© Medullan Inc.

page | 7

New Opportunities: Apple ResearchKit

You're already carrying a powerful medical research tool.

Hundreds of millions of people around the world have an iPhone in their pocket. Each one is equipped with powerful processors and advanced sensors that can track movement, take measurements, and record information — functions that are perfect for medical studies. The sheer number of them being used across the globe opens up new possibilities for researchers. With ResearchKit, researchers can easily create apps that take advantage of iPhone features to gather new types of data on a scale never available before.

Image: Retrieved from Medium (2015). "Apple ResearchKit: A Game Changer for Outcomes Research?" (12 August)

Predictive analytics in healthcare can be used, for example, to help doctors utilize data from Electronic Health Records (EHRs) to produce better models than currently available.[xxvi] A UK hospital shared data on about 1.6 million patients with Google's DeepMind to develop and refine an app called Streams, an alert diagnosis and detection system that can spot when patients are at risk of developing acute kidney injury. In July 2017, ICO ruled the Royal Free NHS Foundation Trust, which oversees hospitals in the UK, failed to comply with the Data Protection Act when it provided patient data to DeepMind.[xxvii]

Even though AI, IoT, and IoLT devices like portable genetic sequencers will significantly impact the ability to create large precision medicine datasets, patients still lack control and ownership of their personal health information.[xxviii] Imagine that patients could utilize a portal to access all of their health records from every time they've been to the doctor or hospital. What would it be like to have access to our entire medical histories in a single platform? By supplementing health records collected by traditional practitioners, patients could sync their data from their Fitbit and their 23andMe DNA profile, and then decide to make all, or some, of their data available to researchers or their primary care provider.[xxix] iCarbonX, a personal health company based in China, aims to provide a platform for continuous monitoring of your health and suggest adjustments to your diet and behavior as the ultimate preventive medicine tool. “But for Jun Wang,” the co-founder of iCarbonX, “it’s not just about treating disease. It’s also about what might be termed personalized health.” ‘Right now you don’t know about your temperature, or your pulse, or the microbes inside you that affect you emotions,’ he says. ‘”[xxx]

Personal health data privacy concerns are intertwined with smart city IoT and IoLT devices. Imagine smart city technology that optimizes patient data to match organ donors with transplant recipients. While this technology would help with the global organ shortage, citizens and patients would be vulnerable to cyberattacks that leak personal health information for profit. This isn’t unheard of; over 200,000 Malaysian organ donors were notified that their personal information including the donor’s name, identification card number, race, nationality, address, and phone numbers were leaked online.[xxxi]

Affective IoT

IoT devices enhanced with affective computing software are also emerging alongside smart city technologies, which have led to a variety of privacy concerns, including the privacy of children and individuals in the justice system. Affective IoT devices like the My Friend Cayla smart doll sent voice and emotion data to the cloud, which led to a US Federal Trade Commission complaint and a ban in Germany.[xxxii] And affective computing algorithms have already appeared in the courtroom to detect remorse and help determine the risk of recidivism.

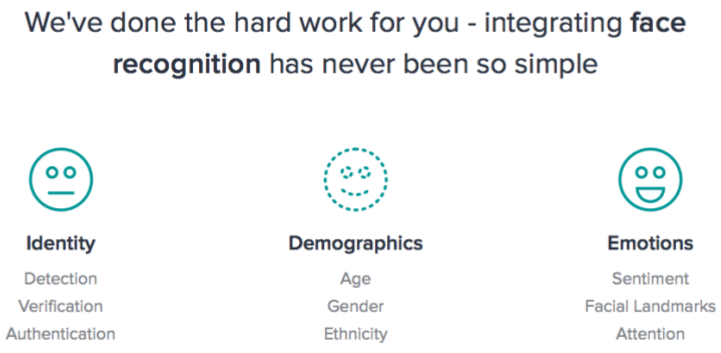

We've done the hard work for you - integrating **face recognition** has never been so simple

Image: Captured from Karios homepage on 3/19/2018.

Karios, an US-based affective computing company, uses facial recognition technology to perform what they call ‘Human Analytics’. Features of this human data optimization platform include: face detection, face identification, face verification, emotion detection, age detection, gender detection, multi-face detection, attention measurement, facial features, sentiment detection, face grouping, and ethnicity detection. Karios’ tagline is quite apt – “Identity, emotions, and demographics all in one place.”[xxxiii]

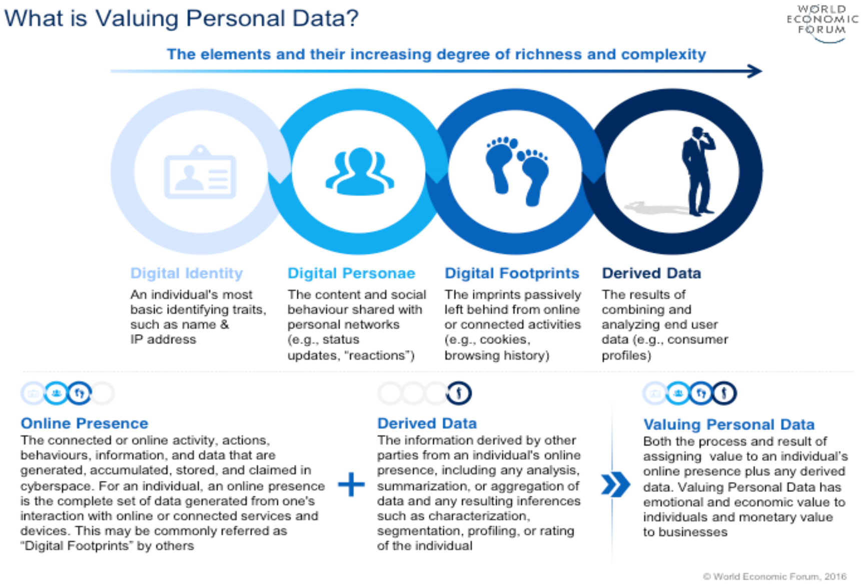
In China, Emotibot “supports a full set of language, image, voice human-computer interactions. Combined with customized development based on the devices and

> scenarios, it enables intelligence devices to have a smart AI brain." According to their website, Emotibot has been used to enhance e-commerce experiences and to identify pain levels. CrowdEmotion, a UK-based affective computing company, "humanizes technology to understand who we are and how we feel." The company developed CloudEmotion, an API that enables developers, academics, and businesses to explore emotional measures across different industries and cultures by providing access to their machine-learning processes for tracking micro-facial expressions and linking them to emotions on Github.

Although predictive intelligence could increase collective security and overall wellbeing, capturing, transferring, and storing the vast amounts of data necessary for smart city AI and affective computing IoT/IoLT devices to function well is always a security risk. Yet, little attention has been paid to how the convergence of AI, IoT, and IoLT within the City Brain and the fourth industrial revolution will impact privacy. While the optimization and ranking of citizen data seems straight out of *Black Mirror*, it's a new reality in China, where privacy is a luxury afforded to few. Though privacy is legally protected in the US, citizens' data is still vulnerable to massive cyberattacks such as the Equifax data breach – with little recourse. In India, the government has mandated compliance with the creation of a country-wide DNA database as part of Aadhaar's identification profile. These examples of intrusive omnipresent and omniscient computing in our daily lives have significant implications for personal privacy and the security of the collective. Who is charged with protecting your privacy? Can the City Brain be hacked? If so, do you have any legal standing to hold the state or data monopolies accountable for failing to protect your data? What does personal privacy look like in a smart city? How do we ensure governments, data monopolies, and non-state actors cannot misuse these optimization technologies?

Privacy in the Fourth Industrial Revolution

The digital age is already changing our notions of privacy. Google, Apple, Facebook, and Amazon (GAFA) comprise what some have called the tech oligopoly - these data monopolies are global in scale and have curated incredible amounts of data on its users. The World Economic Forum created *The Valuing Personal Data Framework* to outline the different elements of our digital avatars and how they are connected.



Digital Identity: An individual's most basic identifying traits, such as name & IP address

Digital Personae: The content and social behaviour shared with personal networks (e.g., status updates, "reactions")

Digital Footprints: The imprints passively left behind from online or connected activities (e.g., cookies, browsing history)

Derived Data: The results of combining and analyzing end user data (e.g., consumer profiles)

Online Presence: The connected or online activity, actions, behaviours, information, and data that are generated, accumulated, stored, and claimed in cyberspace. For an individual, an online presence is the complete set of data generated from one's interaction with online or connected services and devices. This may be commonly referred as "Digital Footprints" by others

Derived Data: The information derived by other parties from an individual's online presence, including any analysis, summarization, or aggregation of data and any resulting inferences such as characterization, segmentation, profiling, or rating of the individual

Valuing Personal Data: Both the process and result of assigning value to an individual's online presence plus any derived data. Valuing Personal Data has emotional and economic value to individuals and monetary value to businesses

© World Economic Forum, 2016

The top cited privacy concerns related to AI and other converging technologies are: lack of understanding of fundamental concepts such as one's online presence and data derived across the general online population; implicit and/or reluctant consent; lack of control over personal data and privacy; deceptive use of terms and conditions agreements; and trading privacy for free services.[xxxiv]

Revelations about the extent of digital mass surveillance have raised questions around the extent to which international legal standards and national mechanisms sufficiently protect individuals from privacy breaches. To frame this discussion, it is important to understand current notions of privacy and how the fourth industrial revolution will affect these conceptions. Here, we will hone our focus to three countries and regions: China, the United States (US), and the European Union (EU). These case studies will be juxtaposed with their respective notions of privacy and compared against the leading privacy regulation – the EU General Data Protection Regulation (GDPR). Finally, we will move into a discussion of the implications for privacy garnered by the increasing implementation of AI technology.

Emerging Technologies & Data Protection Governance

New developments will continue to test governance, including how behavioral and psychological data fits into privacy schemes. Integrating more types of data into the IoT and AI analysis will exacerbate such issues as new links are found between consumer data and health, behavior, and genomic data. If genomic sequences are known from birth, or even screened prior to IVF implantation,[xxxv] then DNA can become data for AI to analyze against other types of personal data aggregated from the IoT.

Technology is pressuring privacy governance systems, testing their outer boundaries.[xxxvi] Developments in data optimization using IoT devices[xxxvii] and the emergence of new type of data – genomic, neural, etc. – present new challenges to securing personal privacy.[xxxviii] Emerging technologies, big data, and their applications apply stress to existing frameworks of data protection governance. In January, reports surfaced of the Strava athletics app revealing the locations of foreign military installations, and possibly individuals, solely based on running data collected and shared from participants who consented to use the app using location tracking.

> The price of innovation does not need to be the erosion of fundamental privacy rights.”
>
> – Elizabeth Denham, UK Information Commissioner

The US and EU frameworks respond to these challenges in different manners, the US with responsive enforcement and industry self-regulation and the EU with a broader, preventive approach. Data optimization and sharing tests the limits of both the US system, which relies on industry self-governance since no statute holistically covers the subject, and the EU approach, which allows for data collection and processing if and only if valid consent is obtained. Ultimately, new technological developments will challenge both approaches and will require new tools to address the subsequent privacy issues.

Further challenges will occur when privacy conflicts with national security interests, as is the case with the UK’s new jihadist content identification tool. Both the US and EU systems may applaud this AI intervention, but ceding individual privacy to collective security may result in user profiling and discrimination by AI technologies. Weighing privacy against promoting public health could present similar complications, including decisions to release identifiable heath data to AI companies for analysis and generation of new health services.[xxxix] When Google’s DeepMind was given patient data from healthcare providers in London without consent of the patients, concerns arose about consent and the extent that AI-powered public health could be prioritized above privacy. Appropriate de-identification, if even possible, may allow such exchanges to occur in the US under HIPAA, and public health or research exemptions may apply under the GDPR.[xl]

Yet, finding the balance between competing values, including promotion of public health or national security and privacy, will be critical as innovations in data collection, aggregation, and analysis continue to open new possibilities. Unanswered questions about how technology challenges privacy raise novel ethical dilemmas,[xli] possibly resulting in new forms of discrimination and profiling with individuals having limited control over their data.[xlii] Ultimately, current privacy governance frameworks are likely insufficient to capture the effects of emerging technologies, and further ethical guidance may be required to fill gaps in oversight.[xliii]

Privacy Governance

As AI, IoT/IoLT, and other emerging technologies continue to influence society and perceptions of privacy,[xliv] innovations in oversight will be required to match progress in technology. Effective governance approaches for personal data require substantial coordination between public and private institutions, and various jurisdictions have crafted frameworks to handle personal data oversight.[xlv] However, conceptualizations of privacy vary by jurisdiction and by culture.[xlvi] The differences are perhaps most pronounced between the decentralized US and more holistic EU frameworks for personal data regulation. Each system offers a different response to privacy issues generated by emerging technologies, though new governance and ethics tools will be required as these technologies outpace existing controls.[xlvii]

China: Globally Sourced Privacy Protection

Privacy as the right of an individual is an imported concept for modern China. Chinese scholarship has historically emphasized personal duties within the family and separately duties to the country, instead of individual rights and selfhood. The Chinese word “Yinsi”, the translation of “privacy”, initially carried negative notions of “secrets to hide”. [xlviii] The Constitution of the People’s Republic of China (PRC), first adopted in 1954, protects personal dignity and the private homes of citizens from violation, and it gives legal protection to the freedom and secrecy of correspondence of citizens.[xlix] Yet, without supporting legislations and judicial actions, the Constitution had little applicability in protecting individual privacy.

As China started its economic reform and global integration in the 1980s, the notion of privacy protection gradually gained social and legal recognition. In 1988, the Chinese Supreme People’s Court (SPC) first issued a judicial interpretation[l] of the General Principles of Civil Law that stipulated a liability for unauthorized disclosure of an individual’s privacy or defamation of one’s character, when it infringes upon the individual’s reputation.[li] A number of new laws and regulations passed in the late 1990s and the 2000s stipulated the obligation for public and private agencies to safeguard personal information during data collection and processing in various contexts, such as medical records, bank accounts and identity cards.[lii] The enactment of Tort Liability Law in 2010, the first comprehensive tort law adopted by China, formally recognized the right of privacy as an independent civil right, and violation of privacy as an actionable tort.[liii]

In the past decade, we have witnessed explosive adoption of information technology in China – and with it steady improvement in legal recognition of citizens’ rights to personal information. For instance, the Standing Committee of the National People’s Congress (NPC) adopted the Decision on Strengthening Protection of Online Information, which has the same legal authority as a law. The primary purposes of the Decision are to protect citizens’ personal online information and online privacy and to safeguard public interests.[liv] The 2013 amendment to the Law on the Protection Consumer Rights and Interests recognized consumers’ rights to protection of personal information during purchase and use of goods and services, and the obligation of enterprises to gain consumers’ consent to collect and use personal information and to safeguard consumers’ personal information. [lv] The Criminal Law amendment in 2015 expanded the criminal liability for illegal sale and provision of personal information (maximum punishment of seven years in prison), for the violation of cybersecurity and other types of cyber-related crimes, and for Internet service providers failing to fulfill duties of network security management. [lvi]

The Cybersecurity Law enacted in 2017, devoted Chapter 4 to protecting personal information from network-based risks.[lvii] In accordance with the law, network providers must obtain data subjects' informed consent to the collection of their personal information, regardless of the prospective uses or the types of data processing. It also for the first time defines "personal information" as information that identifies a natural person either by itself or in combination with other information, in either electronic or in any other form, including a person's name, address, telephone number, date of birth, identity card number and biometric identifiers. "A set of accompanying measures, standards and guidelines are also underway. For instance, the "Information Security Technology - Personal Information Security Specification" (Personal Information National Standards), effective on May 1, 2018, specifies best practices for the collection, retention, use, sharing and transfer of personal information and handling of information breaches. It includes a much more sweeping, risk-based definition of "sensitive" personal information as "any personal information, which, if lost or misused, is capable of endangering persons or property, easily harming personal reputation and mental and physical health, or leading to discriminatory treatment." [lviii] Although this is only a voluntary guideline, it sets benchmarks for future laws and mandatory standards. Compliance will also be instrumental for businesses in China to show cooperation with the Cyberspace Administration of China (CAC). It brings Chinese data privacy framework much closer to the centralized EU approach under GDPR, as opposed to the more decentralized legal framework in the US.

Yet, key issues remain in this nascent governance framework. Firstly, a comprehensive law that defines and protects personal privacy from intrusion by public agencies, private enterprises, and third parties with broad applicability across economic sectors, is still in development. A draft for the Law of Protection of Personal Information was first proposed to the NPC in 2005, and despite numerous attempts, it remains a draft in progress in 2017.[lix]

Secondly, existing rules do not mandate companies to disclose their management of consumer data. As a result, it is up to the private sector to voluntarily provide such disclosure and transparency – which they do not always offer willingly. For instance, according to Ranking Digital Rights, Baidu provided little public disclosure about how long they retain user information, the type of user information they collect, how requests for user information from government and other private companies are handled, and how to address data breaches.[lx] Tencent provided strong disclosure of the type of user information it collects and how it addresses security vulnerabilities, but almost nothing about how long it retains user information and how it handles information requests.[lxi]

Thirdly, there is very little regulation for government agencies in data collection and monitoring, interagency data sharing within public agencies, and data sharing with the private sector. No special law restricts government power to conduct Internet surveillance.[lxii] The National Security Law and the Anti-Terrorism Law, both adopted in 2015, upheld the state power to access and scrutinize information relevant to national security and public interests. As the country starts rolling out a Social Credit System that assesses the trustworthiness of citizens empowered by AI and big data, some administrative rules exist at the local government level on data collection and management practices. Yet overall there is very little regulation on the secondary use of data by agencies, citizen's rights to access and correct data, or third-party access to personal credit data. [lxiii] While China's legal protection for privacy looks inadequate compared to its rapid adoption of AI, big data and IoT technologies, social contexts may explain the public tolerance, or ambivalence, towards the almost free rein of data collection and management empowered by algorithms and big data analytics.

Social Context of Privacy Governance in China

Firstly, the traditional cultural affinity towards collectivism and social welfare, as opposed to individualism, is still strong, and the sheer scale of the population makes AI-enabled security and social services appealing to the public. Unlike western societies where privacy is viewed as an "intrinsic good", privacy in China evolved as an "instrumental good" whose value is derived from the end goal (for instance, social progress and harmony.) [lxiv] Of the world's 31 megacities (10 million inhabitants or more), China alone has six. [lxv] The urbanization trend is only intensifying, posing enormous challenge to governance. The public has largely welcomed the use of big data and AI technologies in fighting rampant crimes such as child trafficking [lxvi] , and streamlining social services.	Secondly, Chinese ICT market has been highly competitive where companies moved faster than regulations to capture markets. As the creation and enactment of regulations and laws have historically lagged technology development, developers have been conditioned to build products and features first and worry about privacy later. [lxvii] In addition, the less educated and the rural population have relatively less awareness of personal data protection compared to the early adopters (tech-savvy young urban consumers), yet they are the driving force behind the rapid expansion of technologies such as mobile payments and online shopping nationwide.	Thirdly, the Communist party legacy of maintaining a lifetime personal dossier ("dang'an") for everyone has led to the public default assumption of the government tracking personal events and use of data. The dossier is a Mao-era system for recording a person's performances in schools and at work by teachers, supervisors and party officials, since all schools, enterprises and agencies used to be government-affiliated entities with party committees. The dossier plays a decisive role in employment, social security and welfare provision. Thus, the government use of personal data empowered by AI may be viewed as a "smart" extension of the existing system.[lxviii]	Fourthly, the contention between the right to privacy and the freedom of information and public speech is an ongoing struggle. The public demand for open data in the provision of social services such as housing has resulted in the disclosure of personal information, such as ID cards and phone numbers, in some cities. The rise of "human flesh search" ("renrou"), citizens banding together to uncover a person's identity and personal information, has gained popularity in fighting corruption, and shaming the "immoral" such as celebrity scandals; yet without legal vigilance such practice can easily cross into cyberbullying and invading personal space.

United States: HIPPA and GINA

Privacy governance in the US takes a softer approach to safeguarding personal data than the EU framework. American culture generally places less significance on the value of privacy than the EU,[lxix] and the text of the US Constitution lacks any explicit mention of or guarantee to privacy. The US Supreme Court has since recognized that privacy exists as an implied right tied only to existing constitutional privileges.[lxx] While American criminal law recognizes individual's protection of a "reasonable expectation to privacy,”[lxxi] this doctrine is limited to government intrusions on privacy and more rooted in shifting social perceptions of privacy than an abstract privacy right.[lxxii]

The US has not linearly progressed towards increasing privacy protection.

With a weak constitutional setting for privacy, the US oversight of data protection relies primarily on a piecemeal legislative approach. [lxxiii] Comprehensive legislation to provide consumer data protection and privacy was proposed under the Obama Administration,[lxxiv] but buckled under poor stakeholder support.[lxxv] At present, privacy governance in the US comes from multiple statutes creating limited privacy controls in certain subject matters. Prominent federal statutes that affect personal data collection, access, and disclosure include: the Financial Services Modernization Act (Gramm-Leach-Bliley Act), the Electronic Communications Privacy Act (ECPA), the Health Insurance Portability and Accountability Act (HIPPA), and the Children’s Online Privacy Protection Act (COPPA). Unique among these privacy laws are statutes such as the Genetic Information Nondiscrimination Act (GINA), which prohibits the use of personal data in insurance coverage and employment decisions, rather than on collecting and disclosing that data.

The scattered statutes controlling personal data protections in the US create a more decentralized and responsive approach to privacy oversight, focused primarily on data collection and disclosure.[lxxvi] Several federal agencies use individual statutes to oversee data protection depending on subject matter,[lxxvii] creating multiple privacy regulators in the US instead of a central oversight body. Legislation also limits regulators to monitoring breaches in personal data use in specified areas, leaving gaps in oversight and only allowing retrospective checks. Such gaps are partially filled by industry self-regulation with varying degrees of success.[lxxviii] Notable examples of policies diluting privacy include the 2001 USA PATRIOT Act and the 2017 repeal of Federal Communications Commission (FCC) rules that would have restricted Internet companies from collecting and selling consumer data.[lxxix] These examples demonstrate US decision-makers’ willingness and struggle to balance privacy protections against other goals, including national security, foreign policy, and industry interests.[lxxx]

European Union: GDPR

Oversight of privacy in the EU adopts a more holistic, centralized method than the US system. A fundamental right to privacy is enshrined in foundational EU law,[lxxxi] providing a platform for broader personal data protections. European courts have consistently upheld these privacy rights.[lxxxii] In 2015, the EU made a landmark decision to reform and expand data protections when enacting the General Data Protection Regulation (GDPR), supplanting the previous Data Protection Directive.[lxxxiii] Enforcement of the GDPR begins in May 2018 and enforcement reaches beyond the EU to the US and other jurisdictions.[lxxxiv]

The GDPR still allows regulators to balance privacy rights against national security interests, but offers little opportunity to balance privacy against industry interests.

The GDPR applies general privacy rules to a broad range of data types regardless of industry type, rather than the US system of creating separate regulations by subject matter and only covering specific types of data.[lxxxv] The new rules will require explicitly consenting consumers for each intended primary and subsequent use of their personal data, allow consumers to retain some control over data following collection, and mandates data handlers to assign “data protection officers” and promptly inform regulators of data breaches.[lxxxvi] Regulation should be centralized and noncompliance can result in administrative fines of up to 4% of global profits. Oversight places obligations on both data controllers, entities that decide how personal data will be used, and data processors, the groups that work with that data.[lxxxvii] The GDPR still allows regulators to balance privacy rights against national security interests,[lxxxviii] but offers little opportunity to balance privacy against industry interests. In this way, the EU takes a more precautionary approach to privacy standards, exemplified by data protection by design provisions.[lxxxix] One potential implication of the EU's approach to data privacy and security is that it could hinder economic competition or create innovations at different speeds and scale. But, at the same time, a precautionary approach to data privacy and security also defends a certain set of values (i.e., privacy is a human right and must be protected through law) in order to provide concrete mechanisms to preserve privacy and security in the age of AI.

The inherent differences between US and EU privacy governance systems have created tensions between regulators and stakeholders. The "Safe Harbor" agreement was established under old EU privacy laws to aid US entities in complying with EU standards.[xc] However, EU courts voided the agreement over concerns that US entities failed to provide sufficient privacy protections.[xci] The Privacy Shield was negotiated to replace Safe Harbor and allow ongoing data transfer between the jurisdictions.[xcii] Ongoing tensions manifest in US corporations expressing apprehension about the GDPR enforcement, its broad impacts, and the potential for large administrative fines under the GDPR.[xciii] The EU historically has shown disapproval of GAFA's technology titans (Google, Apple, Facebook, Amazon) and their data monopoly,[xciv] often citing privacy and data protection violations,[xcv] and the GDPR's implementation may exacerbate these conflicts.

Non-Stigmatization in a Post-Privacy World

While our legacy systems are discussing the adaptation of privacy mechanisms, they struggle keeping pace with emerging and transformative technologies that foster a new form of "surveillance capitalism".[xcvi] With AI and IoT/IoLT devices constantly monitoring our movements, interactions, health, bank statements, and behaviors, privacy may soon become a notion of the past. What if privacy becomes a luxury only few can enjoy? Kenneth Roth, Executive Director of Human Rights Watch, says that privacy should not be limited to those who can afford to protect themselves. "We should protect everyone, not just the rich."[xcvii] While there may be significant benefits from the widespread use of our data in a post-privacy world, "hidden biases in both the collection and analysis stages present considerable risks, and are as important to the big data equation as the numbers themselves."[xcviii]

With the rise of cryptocurrencies and smart contracts, blockchain is becoming a new potential data privacy mechanism – successfully ensuring the immutability of our personal data, such as money transfers, electronic patient records, and legal contracts. Yet, while blockchain may safeguard data anonymity to some extent, it is not necessarily a reliable solution to privacy in the age of ever-increasing proliferation of technology. This is primarily due to the nature of blockchain – it does not apply in all circumstances where privacy may be vulnerable. The blockchain architecture approaches interoperability between AI, IoT, and IoLT systems through centralization of data; but data centralization does not necessarily always lend to the protection of privacy. Although some have speculated that, "blockchain has the necessary features to administer cloudminds including privacy, security, monitoring, and credit-tracking,"[xcix] fundamentally a digital leger keeps track of transactions, therefore blockchain is not well suited for the job of protecting us from AI-enhanced personal surveillance. Some also argue that you shouldn't fear post-privacy if you have "nothing to hide"; others maintain that even if you have nothing to hide, your data can be operationalized against you.[c] The privacy-security quagmire is a result of governments and militaries realizing the power of civilian technologies.

> For the moment at least, we are all living our personal lives in public.
>
> – Gary Younge (2012), *The Guardian*

Data monopolies like Alibaba, Google, 23andMe, and Aadhaar are tasked with protecting the data they collect on us. Yet, these monopolies are also operationalizing our personal data to promote products, track our every move, and curate enormous DNA databases – with or without our informed consent. Even more disturbing, data monopolies are also our last line of data security defense – creating conflicts of interest on a global scale. We are already seeing the post-privacy curtain slowly being lowered as our interaction on platforms such as Facebook, Twitter, and Instagram rise. That unfortunate picture you wish you had not taken will be passed around to everyone you know and some you don't. The fourth industrial revolution is ushering in a post-privacy world characterized by a total transparency. Yet, total transparency still requires reflections on how AI innovation could promote non-stigmatization. Transparency does not solely constitute ethical AI – just because everything, and everyone, would exist in public doesn't mean stigmatization miraculously disappears. On the contrary, there might be even more data that stigmatizes minority groups. For instance, even if China were transparent about its use of AI for surveillance, and subsequent oppression of minority groups, would the international AI community be able to adequately respond?

Before we enter the post-privacy world of total transparency, we need to answer questions like: What does data governance look like in the post-privacy world? How might we protect public data from interference or misuse by governments, non-state actors, and data monopolies? Will there be any legal protections for breaches in data security? Will notions of privacy cease to exist in the post-privacy world entirely? Or, will privacy evolve and adapt? How might we protect against data discrimination in the post-privacy world?

RECOMMENDATIONS

Consider Advancing Non-Stigmatization Tools

Data governance is the appropriate entrance-point for non-stigmatization tools. In preparation for the post-privacy world, it is imperative that we collectively define AI values so we can develop adequate non-stigmatization tools. But, what would AI non-stigmatization tools look like? What would they do? *How* would they work? Blockchain technologies could be a potential tool to curb stigmatization, as they encrypt (i.e., de-identify) data transactions on a digital ledger. While blockchain may be a (somewhat) protected digital ledger tool, it is unclear how it would affect data stigmatization. Though blockchain is, at its core, an encrypted, and thus de-identified, digital transaction ledger, recent cryptocurrency hacks have shown blockchain isn't as secure as previously thought. More research is required to assess the effectiveness of blockchain as a potential non-stigmatization framework. Following the move to the post-privacy world of total transparency, everything and everyone will be traceable.

Increase Public Awareness and Legal Protection of Personal Privacy and Collective Data Security

Campaigns to increase public awareness of the issue and the legal protections afforded to citizens may help achieve this goal. Research has shown that the Chinese public has low trust in privacy protection for internet-connected technologies (ICT-enabled services) and rising awareness of using common sense to privacy protections. [ci] Yet the technical understanding of personal data (such as authorization of location tracking and informed consent) and the adoption of technical countermeasures (such as "do not track" in web browsing) is low, particularly among women, the elderly, and the less educated.[cii] As such, the US should encourage more public diplomacy efforts of technical education on privacy protection and bolster the awareness of average citizens of their rights and choices.

However, questions remain as to how, and if, it is possible for humans to develop non-stigmatization tools for machines. If we are to successfully non-stigmatize data, and humans are capable of this task, then AI cannot discriminate based on sexual orientation, race/ethnicity, sex/gender, social and economic class, health /genetics – or anything else for that matter. If data were non-stigmatized, then would it still be possible to target advertisements to specific groups? Should we enact legislation to prohibit data discrimination?

Avoid Conflicts of Interest in Protecting Privacy

Engage Industry and Government in New Dialogue on Personal Privacy and Collective Data Security

As we mentioned in this brief, there seems to be a conflict of interest for data monopolies like GAFA to protect personal privacy and act as the last line of defense for collective data security. To avoid such conflicts, industry must engage with the government and the public in a new dialogue on privacy that focuses on defining values and balancing personal privacy, collective security, with economic competitiveness. For instance, the unique context of Chinese society in transition means that directly importing legal frameworks for privacy from elsewhere may not be optimal. An approach that considers both the international norms and the country's social context will enhance long-term engagement.

Develop International Data Investment, Trade, Privacy, and Security Standards

Incorporating privacy discussions in the development of international standards and in investment and trade dialogues may help government and data monopolies avoid such conflicts of interest. Chinese companies are venturing globally and practicing self-governance in areas where legal framework is lacking, thus engaging them and the regulators in trade and investment dialogues can help steer the private sector towards international best privacy and security practices. The US also needs to partner with its allies such as the EU to promote privacy discussions in bilateral dialogues with China. The EU-China Smart Cities Dialogue already exists, and the US needs to be more engaged in this long-term international discussion.

Support Collaboration Between Industry, Government, and Ethicists

The way forward is to collectively define a responsible governance of AI and data-optimization for our democracies. Technologists, policymakers and civil societies need to collectively construct what transparency, accountability, civilian safety, and social good means in the algorithmic age. Only then will we be able to determine *how* to design technologies for the common good.

Encourage Constant Improvement of Legal Frameworks

The US can encourage public diplomacy by engaging Internet companies, industry associations, legal scholars, and ethicists worldwide in discussions about better legal frameworks for privacy protection. China's draft Personal Information Protection Law that applies across sectors and all kinds of data, if enacted, may serve as a general data protection law for China.

Assess Impact of the Values in the GDPR on Economic Competitiveness

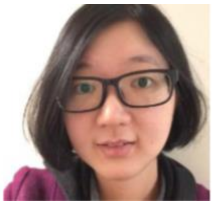
Ethicists and policymakers should engage in substantive discussions with industry and government on how the values within the GDPR might affect economic competiveness in AI innovation. As we have stated in this brief, data governance must balance privacy and security in the AI economy. It is also of the upmost importance that technologist receive technical education on protecting personal privacy and bolstering collective data security.

Commission Report for Further Investigation

Research on the misuse of AI is currently gaining traction[ciii], but little literature exists on how industry, government, policymakers, and ethicists might work together to develop non-stigmatization tools for the post-privacy world. This focused research would benefit various stakeholders as AI innovation continues.

Eleonore Pauwels is the Director of the AI Lab with the Science and Technology Innovation Program at the Wilson Center. She is a writer and international science policy expert, who specializes in the governance and democratization of converging technologies. Leading the AI Lab, Pauwels analyzes and compares how transformative technologies, such as artificial intelligence, genome editing, blockchain and cyber-bio-security, raise new opportunities and challenges for health, security, economics and governance in different geo-political contexts. She analyzes the promises and perils that will likely arise with the development of AI civil and military technologies, the Internet of Living Things and future networks of intelligent and connected bio-labs.

Sarah W. Denton is a research assistant with the Science and Technology Innovation Program at the Wilson Center and the Institute for Philosophy and Public Policy at George Mason University. Her research primarily focuses on ethical and governance implications for emerging technologies such as artificial intelligence, neurotechnology, gene-editing technology, and pharmaceuticals.



Dr. Yujia He was an intern for the Science and Technology Innovation Program at the Wilson Center in 2017. She is now a visiting fellow at the Atlantic Council's Scowcroft Center for Strategy and Security. She has a PhD in International Affairs, Science, and Technology (IAST) and an MS in international affairs from Georgia Tech, BS in chemistry from Peking University, and Stanford Program in Beijing certificate.

Walter G. Johnson completed a research assistant internship in the Science and Technology Innovation Program at the Wilson Center. He is currently a JD candidate at the Sandra Day O'Connor College of Law at Arizona State University (ASU 2020), and previously received his Master of Science and Technology Policy (2017) and B.S. in Chemistry (2015) at ASU.

[i] Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, Paul Scharre, Thomas Zeitzoff, Bobby Filar, Hyrum Anderson, Heather Roff, Gregory C. Allen, Jacob Steinhardt, Carrick Flynn, Sean O Heigeartaigh, Simon Beard, Haydn Belfield, Sebastian Farquhar, Clare Lyle, Rebecca Crootof, Owain Evans, Michael Page, Joanna Bryson, Roman Yampolskiy, and Dario Amodei. (2018). "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation." (February) p. 9 [https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf.]

[ii] Dana G. Smith (2018). “Brain ‘Pacemaker’ Could Help You Remember Only What You Might Enhance,” *Scientific American* (6 February) [https://www.scientificamerican.com/article/brain-ldquo-pacemaker-rdquo-could-help-you-remember-only-what-you-might-forget/].

[iii] IoT includes devices connected to the Internet such as smart refrigerators, self-driving cars, smart phones, etc. IoLT augments IoT devices with biometrics and genome analytic capabilities such as portable genomic sequencers the size of a USB stick and connected to our smart phones. See: Eleonore Pauwels, (2017). “The Internet of Living Things,” *Scientific American* (25 July) [https://blogs.scientificamerican.com/observations/the-internet-of-living-things/].

[iv] Andreas D. Flouris and Jack Duffy (2006). “Applications of artificial intelligence systems in the analysis of epidemiological data,” *European Journal of Epidemiology* 21(3): pp. 167-70. [https://www.ncbi.nlm.nih.gov/pubmed/16547830].

[v] Lin Tang and Cosmin Deciu (2018). US Patent Application, “Methods and process for non-invasive assessment of a genetic variation,” *Sequenom Inc.* US20180032665A1 (1 February) [https://patents.google.com/patent/US20180032665A1/en].

[vi] Garrett Dunlap and Eleonore Pauwels (2017). “The Intelligent and Connected Bio-Labs of the Future: Promise and Peril in the Fourth Industrial Revolution,” *Wilson Briefs* (September) [https://www.wilsoncenter.org/sites/default/files/the_intelligent_connected_biolabs_of_the_future.pdf].

[vii] Rishi Iyengar (2017). “These three countries are winning the global robot race,” *CNN* Tech (21 August) [http://money.cnn.com/2017/08/21/technology/future/artificial-intelligence-robots-india-china-us/index.html]. Also, see: Yogima Steh Sharma and Prachi Verma (2018). “Artificial Intelligence race with China: Panel to create road map,” India Times (8 February) [https://economictimes.indiatimes.com/news/economy/policy/artificial-intelligence-race-with-china-panel-to-create-road-map/articleshow/62813717.cms].

[viii] Rishi Iyengar (2017). “These three countries are winning the global robot race,” *CNN* Tech (21 August) [http://money.cnn.com/2017/08/21/technology/future/artificial-intelligence-robots-india-china-us/index.html]. Also, see: Yogima Steh Sharma and Prachi Verma (2018). “Artificial Intelligence race with China: Panel to create road map,” India Times (8 February) [https://economictimes.indiatimes.com/news/economy/policy/artificial-intelligence-race-with-china-panel-to-create-road-map/articleshow/62813717.cms].

[ix] For an English translation of China’s “New Generation Artificial Intelligence Development Plan,” see: Graham Webster, Rogier Creemers, Paul Triolo, and Elsa Kania (2017). “China’s Plan to ‘Lead’ in AI: Purpose, Prospects, and Problems,” *New America* (1 August) [https://www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-purpose-prospects-and-problems/]. Also see, Molly McParland (2018). “Could China overtake the US in AI development?” *Global Risk Insights* (8 February) [https://globalriskinsights.com/2018/02/china-artificial-intelligence-market-leader/].

[x] Shweta Modgil (2017). “Watchlist: 10 Indian AI startups to Watch Out For in 2018,” *Inc 42* (27 December) [https://inc42.com/features/indian-ai-startups-2018/].

[xi] Guelzim, T., et al. “Introduction and Overview of Key Enabling Technologies for Smart Cities and Homes.” *Smart Cities and Homes*, Morgan Kaufmann, 2016, pp. 1–16. *ScienceDirect*, doi:10.1016/B978-0-12-803454-5.00001-8.

[xii] Jon Russell (2018). “Malaysia’s capital will adopt ‘smart city’ platform form Alibaba,” *Tech Crunch* (29 January) [https://techcrunch.com/2018/01/29/malaysia-alibaba-city-brain/].

[xiii] (2017). “China’s ‘smart cities’ to number 500 before end of 2017.” *China Daily* (21 April) [http://www.chinadaily.com.cn/china/2017-04/21/content_29024793.htm]

[xiv] Michael Totty (2017). “The Rise of the Smart City,” *The Wall Street Journal* (16 April) [https://www.wsj.com/articles/the-rise-of-the-smart-city-1492395120].

[xv] The United States Conference of Mayors. (2016). *Cities of the 21st Century: 2016 Smart Cities Survey* [https://www.usmayors.org/wp-content/uploads/2017/02/2016SmartCitiesSurvey.pdf].

[xvi] David Ingram (2018). "Factbox: Who is Cambridge Analytica and what did it do?" *Reuters* (19 March) [https://www.reuters.com/article/us-facebook-cambridge-analytica-factbox/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07F].
[xvii] Dave Lee (2018). "UK unveils extremism blocking tool," *BBC News* (13 February) [http://www.bbc.com/news/technology-43037899].
[xviii] Ibid.
[xix] Glenn Cohen and Harry S. Graver (2017). "Cops, Docs, and Code: A Dialogue Between Big Data in Health Care and Predictive Policing," *University at California-Davis Law Review:* Symposia Paper: p. 441. [https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Cohen_Graver.pdf].
[xx] Clare Garvie, Alvaro M. Bedoya, and Jonathan Frankle (2016). *The Perpetual Line-Up*, Georgetown Law Center on Privacy and Technology (18 October) [https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf].
[xxi] Ibid. p. 14.
[xxii] Pranbihanga Borpuzari (2018). "Smart vision: This startup AI-powers CCTV surveillance cameras to understand what it sees," *India Economic Times* (9 January) [https://economictimes.indiatimes.com/small-biz/startups/features/this-startup-ai-powers-cctv-surveillance-cameras-to-understand-what-it-sees-uncanny-vision/articleshow/62424609.cms].
[xxiii] Amitabh Sinha (2017). "Understanding the new DNA tech Bill: All your questions answered," *The Indian Express* (1 August) [http://indianexpress.com/article/explained/simply-put-understanding-the-new-dna-tech-bill-4776304/].
[xxiv] "Announcing the Blockchain Challenge | Newsroom | HealthIT.gov." https://www.healthit.gov/newsroom/ blockchain-challenge. Accessed 14 Jun. 2017.
[xxv] View Winners – CCC Innovation Center." Accessed June 13, 2017. [http://www.cccinnovationcenter.com/ challenges/block-chain-challenge/view-winners/]; "Ethereum: A Secure Decentralised Generalised ... - Gavin Wood." http://gavwood.com/paper.pdf. Accessed 14 Jun. 2017.
[xxvi] Glenn Cohen and Harry S. Graver (2017). "Cops, Docs, and Code: A Dialogue Between Big Data in Health Care and Predictive Policing," *University at California-Davis Law Review:* Symposia Paper: p. 445. [https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Cohen_Graver.pdf].
[xxvii] ICO (2017). "Royal Free – Google DeepMind failed to comply with data privacy law," (3 July) [https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/].
[xxviii] "Announcing the Blockchain Challenge | Newsroom | HealthIT.gov." https://www.healthit.gov/newsroom/ blockchain-challenge. Accessed 14 Jun. 2017.
[xxix] Eleonore Pauwels and Nathaniel Grevatt (2017). "The Social Benefits of Blockchain for Health Data: Securing Patient Privacy and Control," *Wilson Briefs* (5 December) [https://www.wilsoncenter.org/publication/the-social-benefits-blockchain-for-health-data-securing-patient-privacy-and-control].
[xxx] David Ewing Duncan (2017). "Can AI Keep You Healthy?" *MIT Technology Review* (3 October) [https://www.technologyreview.com/s/608987/how-ai-will-keep-you-healthy/].
[xxxi] (2018). "Personal details of over 200,000 Malaysian organ donors leaked online: report," *Reuters* (23 January) [https://www.reuters.com/article/us-malaysia-cybercrime/personal-details-of-over-200000-malaysian-organ-donors-leaked-online-report-idUSKBN1FD07B].
[xxxii] See Katie Collins (2017), "That smart doll could be a spy. Parents, smash!" *CNET* (17 February) [https://www.cnet.com/news/parents-told-to-destroy-connected-dolls-over-hacking-fears/]; Steven Musil and Alfred NG (2016). "Talking toys accused of recording and sharing kids' secrets," *CNET* (7 December) [https://www.cnet.com/news/kids-talking-toys-iot-internet-of-things-privacy-ftc/].
[xxxiii] See Karios' website for more information: [https://www.kairos.com/features].
[xxxiv] Cocorocchia, Claudio. "5 Things You (Probably) Don't Know about Online Privacy – but Should." *World Economic Forum*, 24 May 2017, https://www.weforum.org/agenda/2017/05/your-personal-data-privacy-what-to-know/.
[xxxv] Regalado, Antonio. "Eugenics 2.0: We're at the Dawn of Choosing Embryos by Health, Height, and More." *MIT Technology Review*, 1 Nov. 2017, https://www.technologyreview.com/s/609204/eugenics-20-were-at-the-dawn-of-choosing-embryos-by-health-height-and-more/.

[xxxvi] Abrams, Martin, et al. *Artificial Intelligence, Ethics and Enhanced Data Stewardship*. The Information Accountability Foundation, 20 Sept. 2017, http://informationaccountability.org/publications/.

[xxxvii] Wachter, Sandra. *Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR*. SSRN Scholarly Paper, ID 3083554, Social Science Research Network, 6 Dec. 2017. *papers.ssrn.com*, http://dx.doi.org/10.2139/ssrn.3083554.

[xxxviii] Dyke, Stephanie OM, et al. “Sharing Health-Related Data: A Privacy Test?” *Npj Genomic Medicine*, vol. 1, Aug. 2016, p. 16024. *www.nature.com*, doi:10.1038/npjgenmed.2016.24 [https://www.nature.com/articles/npjgenmed201624.pdf].

[xxxix] Powles, Julia, and Hal Hodson. “Google DeepMind and Healthcare in an Age of Algorithms.” *Health and Technology*, vol. 7, no. 4, Dec. 2017, pp. 351–67. *link.springer.com*, doi:10.1007/s12553-017-0179-1.

[xl] “The Final GDPR Text and What It Will Mean for Health Data.” *Hogan Lovells Chronicle of Data Protection*, 20 Jan. 2016, https://www.hldataprotection.com/2016/01/articles/health-privacy-hipaa/the-final-gdpr-text-and-what-it-will-mean-for-health-data/

[xli] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. “Personal Data and Individual Access Control.” *Ethically Alligned Design, Version 2*, 2017, pp. 83–112, https://standards.ieee.org/develop/indconn/ec/autonomous_systems.html.

[xlii] Ethics Advisory Group, European Data Protection Supervisor. *Towards a Digital Ethics*. 25 Jan. 2018, https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf.

[xliii] Abrams, Martin, et al. *Artificial Intelligence, Ethics and Enhanced Data Stewardship*. The Information Accountability Foundation, 20 Sept. 2017, http://informationaccountability.org/publications/.

[xliv] Helbing, Dirk, and Evangelos Pournaras. “Society: Build Digital Democracy.” *Nature News*, vol. 527, no. 7576, Nov. 2015, p. 33. *www.nature.com*, doi:10.1038/527033a.

[xlv] Salido, Javier, and Patrick Voon. “A Guide to Data Governance for Privacy, Confidentiality, and Compliance.” *International Association of Privacy Professionals*, Jan. 2010, https://iapp.org/resources/article/a-guide-to-data-governance-for-privacy-confidentiality-and-compliance/.

[xlvi] Doneda, D., and V. A. F. Almeida. “Privacy Governance in Cyberspace.” *IEEE Internet Computing*, vol. 19, no. 3, May 2015, pp. 50–53. *IEEE Xplore*, doi:10.1109/MIC.2015.66.

[xlvii] Abrams, Martin, et al. *Artificial Intelligence, Ethics and Enhanced Data Stewardship*. The Information Accountability Foundation, 20 Sept. 2017, http://informationaccountability.org/publications/.

[xlviii] Jingchun, Cao. (2005). Protecting the Right to Privacy in China. Victoria University of Wellington Law Review, 36 (3), 645. http://www.austlii.edu.au/nz/journals/VUWLawRw/2005/25.html.

[xlix] Constitution of the People’s Republic of China (PRC)1954. http://www.npc.gov.cn/wxzl/wxzl/2000-12/26/content_4264.htm Articles 89 and 90 pertained to the protection of personal freedom, private homes and correspondence. They have become Articles 38, 39 and 40 in Chapter 2 of the current Constitution. http://www.npc.gov.cn/englishnpc/Constitution/2007-11/15/content_1372964.htm

[l] Judicial precedents are not enforceable in China, but SPC bears the authority to issue Judicial Interpretations (sifa jieshi) as guidelines to the trials, which are nationally enforceable.

[li] Point 140, Opinions of the Supreme People's Court on Several Issues concerning the Implementation of the General Principles of the Civil Law of the People's Republic of China (For Trial Implementation). http://www.ipkey.org/en/resources/china-ip-law/15-civil-law-procedures/3141-opinions-of-the-supreme-people-s-court-on-several-issues-concerning-the-implementation-of-the-general-principles-of-the-civil-law-of-the-people-s-republic-of-china-for-trial-implementation

[lii] Examples include Law on Practicing Doctors of the People's Republic of China 1999, Law of the People's Republic of China on Resident Identity Cards 2003, Law of the People's Republic of China on Banking Regulation and Supervision 2004.

[liii] Article 2, Tort Liability Law of the People's Republic of China. http://www.cpahkltd.com/EN/info.aspx?n=20110224112237940593

[liv] McDermott Will & Emery. China: Decision on Strengthening the Protection of Online Information. https://www.natlawreview.com/article/china-decision-strengthening-protection-online-information

[lv] See Articles 14 and 29, Law of the People's Republic of China on the Protection of Consumer Rights and Interests

[lvi] Xinhua. (2015, August 29). China Focus: China adopts amendments to Criminal Law. http://www.xinhuanet.com/english/2015-08/29/c_134568394.htm

[lvii] Cybersecurity Law of the People's Republic of China. http://www.lawinfochina.com/display.aspx?id=22826&lib=law

[lviii] Bird & Bird. (2018, January 26). “China Cybersecurity Law update: Personal Information National Standards officially published!”, Lexology, https://www.lexology.com/library/detail.aspx?g=23b69b8e-9240-4cbe-9d9a-ca7a25a36c03. Also see Yan Luo and Phil Bradley – Schmieg. (2018, January 25). “China Issues New Personal Information Protection Standard”, Covington & Burling LLP, https://www.insideprivacy.com/international/china/china-issues-new-personal-information-protection-standard/.”

[lix] Draft for the Law of Protection of Personal Information 2017. http://www.sohu.com/a/203902011_500652

[lx] Ranking Digital Rights. Corporate Accountability Index 2017: Baidu, Inc. https://rankingdigitalrights.org/index2017/companies/baidu/

[lxi] Ibid.

[lxii] James D. Fry, Privacy, Predictability and Internet Surveillance in the U.S. and China: Better the Devil You Know?, 37 U. Pa. J. Int’l L. 419 (2015).http://scholarship.law.upenn.edu/jil/vol37/iss2/1

[lxiii] Chen, Yongxi and Cheung, Anne Sy. (2017). The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System. The Journal of Comparative Law, 12 (2), 356-378. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2992537

[lxiv] Lü, Yao-Huai. (2005). Privacy and data privacy issues in contemporary china. Ethics and Information Technology 7 (1):7-15. https://link.springer.com/article/10.1007%2Fs10676-005-0456-y

[lxv] UN. (2017). The World’s Cities in 2016. http://www.un.org/en/development/desa/population/publications/pdf/urbanization/the_worlds_cities_in_2016_data_booklet.pdf

[lxvi] Reuters. (2017, February 4). Mobile App Helps China Recover Hundreds of Missing Children. https://www.reuters.com/article/us-china-trafficking-apps/mobile-app-helps-china-recover-hundreds-of-missing-children-idUSKBN15J0GU

[lxvii] Lockett, Hudson. (2015). In-depth: Chinese e-commerce's rush into online finance could put countless users' data at risk. China Economic Review. https://chinaeconomicreview.com/chinese-e-commerces-rush-online-finance-could-put-countless-users-data-risk/

[lxviii] Hollinsworth, Julia. (2017, December 25). Even China’s Backwater Cities Are Going Smart. Sixth Tone. http://www.sixthtone.com/news/1001452/even-chinas-backwater-cities-are-going-smart.

[lxix] Hainsworth, Jeremy. *Global Privacy Ethics Subject to Cultural Differences*. 13 Apr. 2016, https://www.bna.com/global-privacy-ethics-n57982069807/.

[lxx] Griswold v. Conn., 381 U.S. 479, 483–85 (1965); Helscher, David. “Griswold v. Connecticut and the Unenumerated Right of Privacy.” *Northern Illinois University Law Review*, vol. 15, 1994, pp. 33–62.

[lxxi] Cividanes, Paul. “Cellphones and the Fourth Amendment: Why Cellphone Users Have a Reasonable Expectation of Privacy in Their Location Information.” *Journal of Law and Policy*, vol. 25, 2017 2016, pp. 317–56.

[lxxii] Kerr, Orin. “Answering Justice Alito’s Question: What Makes an Expectation of Privacy ‘reasonable’?” *Washington Post*, 28 May 2014. *www.washingtonpost.com*, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/28/answering-justice-alitos-question-what-makes-an-expectation-of-privacy-reasonable/.

[lxxiii] Sotto, Lisa J., and Aaron P. Simpson. “Data Protection & Privacy 2015: Getting the Deal Through.” *Hunton & Williams Privacy & Information Security Law Blog*, 2015, https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2011/04/DDP2015_United_States.pdf.

[lxxiv] “We Can’t Wait: Obama Administration Unveils Blueprint for a ‘Privacy Bill of Rights’ to Protect Consumers Online.” *Obamawhitehouse.archives.gov*, 23 Feb. 2012, https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

[lxxv] Sasso, Brendan. “Obama’s ‘Privacy Bill of Rights’ Gets Bashed from All Sides.” *The Atlantic*, Feb. 2015. *The Atlantic*, https://www.theatlantic.com/politics/archive/2015/02/obamas-privacy-bill-of-rights-gets-bashed-from-all-sides/456576/.

[lxxvi] Jolly, Ieuan. “Data Protection in the United States: Overview.” *Practical Law by Thomson Routers*, 2017, [https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default].

[lxxvii] Sotto, Lisa J., and Aaron P. Simpson. "Data Protection & Privacy 2015: Getting the Deal Through." *Hunton & Williams Privacy & Information Security Law Blog*, 2015, https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2011/04/DDP2015_United_States.pdf.

[lxxviii] Listokin, Siona. "Industry Self-Regulation of Consumer Data Privacy and Security, 32 J. Marshall J. Info. Tech. & Privacy L. 15 (2015)." *The John Marshall Journal of Information Technology & Privacy Law*, vol. 32, no. 1, Jan. 2015, https://repository.jmls.edu/jitpl/vol32/iss1/2.

[lxxix] Lohr, Steve. "Trump Completes Repeal of Online Privacy Protections from Obama Era." *The New York Times*, 3 Apr. 2017. *NYTimes.com*, https://www.nytimes.com/2017/04/03/technology/trump-repeal-online-privacy-protections.html.

[lxxx] Serwin, Andrew. "Striking the Balance—Privacy versus Security and the New White House Report." *International Association of Privacy Professionals*, 19 Dec. 2013, https://iapp.org/news/a/striking-the-balanceprivacy-versus-security-and-the-new-white-house-report/; Shepardson, David. "Trump Signs Repeal of U.S. Broadband Privacy Rules." *Reuters*, 4 Apr. 2017. *Reuters*, https://www.reuters.com/article/usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSL2N1HC21O.

[lxxxi] European Union. *Charter of Fundamental Rights of the European Union art. 7*. OJ C, vol. 83/02, 30 Mar 2010, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12010P&from=EN; European Union. *Treaty of Lisbon Amending Treaty on European Union and the Treaty Establishing the European Community*. OJ C, vol. 306/01, 13 Dec 2007, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ%3AC%3A2007%3A306%3ATOC

[lxxxii] Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, ECLI:EU:C:2014:317, http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-131/12&td=ALL; Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, http://curia.europa.eu/juris/liste.jsf?num=C-362/14.

[lxxxiii] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Data Protection Directive)." *OJ L*, vol. 281, 31995L0046, 23 Nov 1995, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.

[lxxxiv] Blackmer, W.Scott. "GDPR: Getting Ready for the New EU General Data Protection Regulation." *InfoLawGroup LLP*, 5 May 2016, https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/.

[lxxxv] Ibid.

[lxxxvi] Promontory Financial Group. *EU GDPR: Summary of Key Provisions*. 2015, https://iapp.org/media/pdf/resource_center/Promontory_GDPR_compromise.pdf; Gladies, Peter. "A Summary of the EU General Data Protection Regulation." *dataIQ*, 2015, https://www.dataiq.co.uk/blog/summary-eu-general-data-protection-regulation.

[lxxxvii] Information Commissioner's Office (UK). *Data Controllers and Data Processors: What the Differences Is and What the Governance Implications Are*. 2016, https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf; Baker & McKenzie International. "Preparing for New Privacy Regimes: Privacy Professionals' Views on the General Data Protection Regulation and Privacy Shield." May 2016, http://f.datasrvr.com/fr1/416/76165/IAPP_GDPR_and_Privacy_Shield_Survey_Report.pdf

[lxxxviii] Blackmer, W.Scott. "GDPR: Getting Ready for the New EU General Data Protection Regulation." *InfoLawGroup LLP*, 5 May 2016, https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/.

[lxxxix] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance)." *OJ L*, vol. 119/01, 32016R0679, 4 May 2016, http://data.europa.eu/eli/reg/2016/679/oj/eng.

[xc] Weiss, Martin A., and Kristin Archick. "U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield Note." *Congressional Research Service*, Feb. 2016, p. [i]-14.

[xci] Ibid.

[xcii] International Trade Administration, U.S. Department of Commerce. *Privacy Shield Program Overview*. 2018, https://www.privacyshield.gov/Program-Overview.

[xciii] Dwoskin, Elizabeth. “EU Data-Privacy Law Raises Daunting Prospects for U.S. Companies.” *Wall Street Journal*, 16 Dec. 2015. *www.wsj.com*, http://www.wsj.com/articles/eu-data-privacy-law-raises-daunting-prospects-for-u-s-companies-1450306033.

[xciv] Dwyer, Paula. “Should America’s Tech Giants Be Broken Up?” *Bloomberg.com*, 20 July 2017. *www.bloomberg.com*, https://www.bloomberg.com/news/articles/2017-07-20/should-america-s-tech-giants-be-broken-up.

[xcv] Couturier, Kelly. “How Europe Is Going After Apple, Google and Other U.S. Tech Giants.” *The New York Times*, 13 Apr. 2015. *NYTimes.com*, [https://www.nytimes.com/interactive/2015/04/13/technology/how-europe-is-going-after-us-tech-giants.html]; Guinness, Harry. “What Is GAFA? Why the EU Doesn’t Love Large American Internet Companies.” *MakeUseOf*, 18 June 2015, https://www.makeuseof.com/tag/gafa-eu-doesnt-love-large-american-internet-companies/.

[xcvi] See: Zuboff, Shoshana. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30, no. 1 (March 2015): 75–89 [http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754]; and Paul Bluementhal (2018). “Facebook and Google’s Surveillance Capitalism Model is in Trouble,” *Huffington Post* (27 January) [https://www.huffingtonpost.com/entry/facebook-google-privacy-antitrust_us_5a625023e4b0dc592a088f6c].

[xcvii] Spivack, Nova. “The Post-Privacy World.” *WIRED*, July 2013, https://www.wired.com/insights/2013/07/the-post-privacy-world/.

[xcviii] Kate Crawford (2013). “The Hidden Biases in Big Data,” *Harvard Business Review* (1 April) [https://hbr.org/2013/04/the-hidden-biases-in-big-data].

[xcix] Melanie Swan (2016). “The Future of Brain-Computer Interfaces: Blockchaining Your Way into a Cloudmind,” *Journal of Evolution & Technology*, 26:2 (October) [https://jetpress.org/v26.2/swan.htm].

[c] Gary Younge (2012). “Social media and the post-privacy society,” *The Guardian* (2 April) [https://www.theguardian.com/commentisfree/cifamerica/2012/apr/02/social-media-and-post-privacy-society].

[ci] Wang, Zhong and Yu, Qian. (2015). Privacy trust crisis of personal data in China in the era of Big Data: The Survey and countermeasures. *Computer Law & Security Review*, 31, 782-792.

[cii] Ibid.

[ciii] Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, Paul Scharre, Thomas Zeitzoff, Bobby Filar, Hyrum Anderson, Heather Roff, Gregory C. Allen, Jacob Steinhardt, Carrick Flynn, Sean O Heigeartaigh, Simon Beard, Haydn Belfield, Sebastian Farquhar, Clare Lyle, Rebecca Crootof, Owain Evans, Michael Page, Joanna Bryson, Roman Yampolskiy, and Dario Amodei. (2018). "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation." (February) [https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf.]