OpenAccessPub

Journal of Big Data Research

ISSN: 2768-0207

DOI: 10.14302/issn.2768-0207.jbr-21-4048

Review Article

Freely Available Online

Legal, Marketing, and Advertising Issues with Big Data

Donald L. Buresh, Ph.D., J.D., L.L.M.[1,*]

[1]Morgan State University

Corresponding author:

Donald L. Buresh, Ph.D., J.D., L.L.M. Morgan State University

Keywords:

Big Data, Internet advertising and marketing, Privacy, Surveillance capitalism

Received: Dec 22, 2021

Accepted: Dec 26, 2021

Published: Jan 04, 2022

Abstract

The purpose of this essay is to discuss the advantages and disadvantages and the benefits and costs of Big Data. The paper outlines the relevant federal and state privacy laws, including the California Consumer Privacy Act as amended, the Virginia Consumer Data Protection Act, and the Colorado Privacy Act. While highlighting several Federal Trade Commission privacy violation cases, the effects of Big Data collection and government surveillance are described in some detail. Advertising and marketing are defined, where it is argued that while the scanning of emails by email providers may be legal, it should be accomplished with consent, or not at all. The essentials of contract law and specific contract negotiation techniques are outlined for the benefit of attorneys. Finally, it is argued that although Big Data is the wave of the future, like all human institutions, it has in its definition the inherent paradoxes of transparency, identity, power, and exclusion that may potentially spell its undoing.

Introduction

Many centuries and millennia ago, human beings were hunters and gatherers. Food and shelter were plentiful in the summer, but the conditions were harsh during the winter, and food was scarce. About six thousand years ago, humans became farmers and grew crops in the winter, storing food for the winter to come. This situation lasted for thousands of years. The Renaissance began about 700 years ago, people began to gather in cities, and businesses started to flourish. Three hundred years ago, the Enlightenment came on the scene, giving birth to the age of capitalism between 1715 and 1750. The Industrial Revolution was just around the corner.

With the advent of machines, mass production of goods could begin in earnest. There was a reckless dash for innovation, and with it came manufactured goods of every kind and color. With the desire for untold wealth and trade, bloody wars followed, almost as if they went hand in hand. Several years after World War II, computers were born. At first, computers were bulky machines occupying a large air-conditioned room, powered by vacuum tubes and large amounts of electricity. However, as it turned out,

computers became smaller, more powerful, and used less energy with each passing day.

In the late 1970s, microcomputers became commercially available. It was the first time that people of limited means could afford a computer and then create computer programs of their own. These were visionaries who believed that giving people the means to attain the power of knowledge was a leap towards freedom. The Information Age was born out. There was no turning back.

The Information Age has matured with the advent of Big Data. However, instead of empowering people to achieve financial independence, Big Data seems to be the vehicle ensuring that governments and corporations remain the dominant force in society. As advertising and marketing precede the steady, continuous flow of goods and services, it is crucial to understand that Big Data is the medium for the next societal transformation. At this stage of societal evolution, Big Data holds the promise of incessant consumption for those who have the means to ride the Big Data train. As for the rest of humanity, only time will tell what the future holds. Toffler was right when he wrote in 1980 that the Information Age had just begun [1].

Literature Review

The purpose of this literature review is to scrutinize Big Data from various angles. In the literature review, Big Data is defined, followed by a discussion of the relevant federal and state statutes that focus on Big Data and the various law review articles that talk about Big Data in a cybersecurity context. In the fourth subsection, Big Data is examined in light of surveillance and privacy matters surrounding Big Data. The fifth subsection addresses advertising and marketing in general, along with the issues peculiar to big data. The sixth subsection is concerned with contract law and its relationship to Big Data. In the following subsection, specific contractual recommendations are discussed, particularly regarding how attorneys should evaluate potential and existing contracts to assure that Big Data issues are appropriately addressed. Finally, a summary of the literature review encapsulates the information presented in the literature review.

Definition of Big Data

What is Big Data? According to Oracle Inc., Big Data is data that "contains greater variety, arriving in increasing volumes and with more velocity" [2]. This is also known as the three Vs of Big Data. In terms of volume, Big Data processes high volumes of low-density data that is essentially unstructuredv[3]. The data may have an unknown value, such as a Twitter data feed or clickstreams on a web page or a mobile app. For some organizations such as Google or Twitter, Big Data means tens of terabytes or petabytes of data. Velocity is the speed or rate at which data is received and processedv[4]. In Big Data, intelligent products that gather the volumes of data typically operate and evaluate data in real-time or close to real-time. Finally, traditionally, data types were structured and fit conveniently into a relational database. However, with the advent of Big Data, unstructured or semi-structured data types such as text, audio, and video demand preprocessing to achieve meaningv[5].

According to Mayer-Schönberger and Cukier, Big Data is a significant shift in how organizations collect, use, and think about data [6]. The value of Big Data is that it can tease out hidden connections from seemingly unrelated data and thus has the potential of predicting future behavior, possibly violating individual privacy. The authors outline some of the future risks, opportunities, and legal implications for a Big Data society. Marz observed that Big Data has borne a new breed of technologies, including distributed filesystems, the MapReduce computation framework, and distributed locking services pioneered by Google and Amazon [7].

Relevant Federal and State Privacy Statutes

Numerous federal laws affect cyber security and Big Data in one way or another. According to Johnson, the Economic Espionage Act (EEA) of 1996 [8] became law on October 11, 1996 [9,10]. The law deals with industrial

espionage, also known as the knowing misappropriation and subsequent acquisition of trade secrets, where the intent is to profit a foreign government[11]. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a significant cybersecurity law. HIPAA generated national standards to protect sensitive patient health information from being exposed without a patient's consent [12]. The HIPAA Privacy Rule deals with disclosing protected health information regarding individuals by organizations subject to the rule [13].

The Gramm-Leach-Bliley Act (GLBA) of 1999 [14] is another primary cybersecurity law currently in place. It is also known as the Financial Modernization Act (FMA) of 1999 [15] because it addresses how financial institutions control individual private information [16]. The Federal Information Security Management / Modernization (FISMA) is the third primary cybersecurity law in the United States. The FISMA Act of 2002 [17] was included in the E-Government Act (EGA) of 2002 [18,19]. FISMA of 2014 [20] amended FISMA of 2002 by reinforcing the employment of continuous monitoring systems while reducing the overall reporting requirements and focusing an agency on the compliance and reporting of breaches in security [21]. FISMA of 2014 also required the Office of Management and Budget (O.M.B.) to revise O.M.B. Circular A-130, which promoted changes in reporting as technology progressed [22,23].

The Modernizing Government Technology Act (MGTA) of 2018 [24] is vital to the National Defense Authorization Act (NDAA) of 2017 [25] that was passed on December 12, 2017 [26]. The MGTA permitted federal agencies to invest in modern technology that improved the delivery of services to the public, ensuring the security of sensitive systems and data and thus saving taxpayer money [27]. The Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology (SECURE IT) Act of 2019 [28] demanded that the Secretary of Homeland Security to "generate a security vulnerability disclosure policy, to establish a bug bounty program for the Department of Homeland Security, to amend title 41, United States Code, to provide for Federal acquisition supply chain security, and for other purposes [29]." On February 24, 2021, President Biden issued Executive Order 14,017 entitled, *Executive Order on America's Supply Chains [30]*.

Executive Order 14,017 Stated that the

"United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security. Pandemics and other biological threats, cyber-attacks, climate shocks and extreme weather events, terrorist attacks, geopolitical and economic competition, and other conditions can reduce critical manufacturing capacity and the availability and integrity of critical goods, products, and services. Resilient American supply chains will revitalize and rebuild domestic manufacturing capacity, maintain America's competitive edge in research and development, and create well-paying jobs [31]."

Executive Order 14,017 was an administrative policy that synchronized the various Cabinet departments' supply chain security activities from a cybersecurity perspective[32].

The first standard is the European Union's (EU) General Data Protection Regulation (GDPR) [33]. The GDPR is a set of legal guidelines that address collecting and processing personal information regarding individuals who live and reside in the EU [34]. The GDPR applies regardless of where a website is located [35]. Any site accessed by a European citizen must obey the regulation, irrespective of whether an organization markets goods or services to EU residents [36]. The GDPR applies to organizations that do business in the EU.

The second statute is the California Consumer Privacy Act (CCPA) [37]. The CCPA became law on June 28, 2018, when former California Governor Jerry Brown signed SB-375 [38]. The first amendments to the CCPA were passed on August 31, 2018, whereby the CCPA became effective on January 1, 2020 [39]. The purpose of the CCPA was to safeguard the personal information of

California consumers independent of what economic sector the data originated [40]. In the November 2020 election, California passed Proposition 24, or the California Privacy Rights Act (CPRA) [41], by 56 percent [42]. With the CPRA becoming law, California citizens now possess the right to correct inaccurate information, the right to ensure that their collected personal information be subordinate to data minimization and purpose limitations, and the right to receive a notice from businesses that are planning on employing sensitive personal information, along with the right to prevent an organization from using that information [43]. The CPRA expanded the right to access information regardless of when it was collected unless it is impossible or impracticable, the right to opt-out of sharing information with third parties no matter if an individual is a buyer or a seller, and the right to sue a business when the organization exposes user names and passwords [44]. The CPRA will take effect on January 1, 2023 [45].

A third statute is the Virginia Consumer Data Protection Act (VCDPA)[46] which, on March 2, 2021, Governor Ralph Northam signed into law [47]. The fourth statute is Colorado's Privacy Act (CPA) [48] which became law on July 8, 2021 [49]. Nevada [50] and Maine [51] have also passed privacy laws, but these laws are not nearly as comprehensive as the privacy laws in California, Virginia, and Colorado [52].

Various court cases deal with cybersecurity and Big Data, including *In the Matter of TaxSlayer, L.L.C[53].*, *In the Matter of Everalbum Corp [54].*, and the SolarWinds Corp[55]. breach. The first two cases were brought to federal district courts by the Federal Trade Commission (FTC). According to the FTC complaint, TaxSlayer was a financial institution subject to Section 509(3)(A) of the GLBA, 15 U.S.C. § 6809(3)(A) because it provided tax planning and tax preparation services[56]. The company collected non-public personal information as defined by 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1015.3(p)(1)-(3) [57]. Because of these two reasons, TaxSlayer was subject to the GLBA Privacy Rule, and the GLBA Safeguards Rule.

According to the FTC, Everalbum violated Section 5(a) of the Federal Trade Commission Act, or 15 U.S.C. § 45, which states that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, [were] declared unlawful [58,59]." Finally, the SolarWinds attack was a supply chain attack where an adversary inserted malicious code into the company's software application [60]. The attack was compromised of Trojan horses [61], where the placement of a pregnant piece of code permitted hackers to infect hundreds, if not thousands, of computers as SolarWinds provided its wares to its customers [62]. The two FTC settlement agreements and the information gleaned from the SolarWinds breach could be used to create reasonable cybersecurity and Big Data protection standards.

Other Issues with Big Data

Currently, Big Data evangelists are singing the hymns of Big Data, claiming that Big Data will help society make better decisions, conserve precious resources, trace and cure a host of diseases, and ensure that human life is safe, efficient, and possibly even effective [63]. It is undeniable that Big Data can yield substantial future benefits. Big Data is an extraordinary knowledge revolution, yet to be fair and cautious, it is essential to take a step backward and critically examine Big Data independent of the persuasive rhetoric that could be drowning out a more balanced understanding.

According to Richards and King, Big Data suffers from three paradoxes – the transparency paradox, the identity paradox, and the power paradox [64]. The transparency paradox is that Big Data promises to ensure that society is more transparent, yet the collection of massive amounts of data is invisible, where the tools and techniques to collect this mammoth amount of data are opaque, clothed in mystery by layers of physical, legal, and technical privacy seemingly by design. The paradox is that while virtually guaranteeing an insurrection in transparency, Big Data is conducted in a shroud of secrecy [65]. Although there are legitimate arguments for

protecting this clandestine behavior, one cannot help but inquire whether Toto can still pull back the curtain, revealing the Wizard of Oz.

The second paradox discussed by Richards and King is the identity paradox. The identity paradox is essentially a contradiction, where Big Data desires to *identify* yet menaces *identity*. The right to privacy heralds from Warren and Brandeis, who boldly proclaimed over 130 years ago that privacy is the "right to be let alone [66]." The right of identity – to be who one wants to be and to do what one desires to do – is born out of the right of free choice. The issue is that the feedback loops hand-crafted by Google and other Big Data organizations will more than likely steer an individual in the entity's direction, thereby not so subtly violating one's free will. Richards and King imagined that because of the identity paradox, the dystopian outlook depicted in the motion picture *Gattaca [67]* may very well be a glimpse into the future [68]. As expressed by Aldous Huxley when Mike Wallace interviewed him, the erosion of one's freedom may be a Big Data consequence [69].

The third paradox is the power paradox, where Big Data sensors are predominately controlled by influential intermediary persons and institutions, and where the benefits of Big Data flow to the individuals and entities that weld the magic wand of power [70]. The effect of the power paradox is to create patrician winners and plebian losers in society. By not understanding the applicable legal and technical limits, individuals may surrender to a life of silent desperation while governments and corporations do what they want to be the default. According to Richards and King, a precarious state of affairs is the result. Thus, if privacy, transparency, autonomy, and identity are protected by law, the consequences are manifold and negative, particularly when considering the advertising and marketing of Big Data.

Finally, according to Leman, some individuals under Big Data may be excluded from its benefits [71]. In examining the effects of Big Data, Leman posits two people. The first is a thirty-year-old white-collar resident of Manhattan who enjoys all of the benefits of a technological world, including a smartphone, Google Gmail, Netflix, Spotify, and Amazon. This individual employs the default settings on Facebook to maintain close contact with friends. This individual tweets and posts photographs on Flickr and Instagram and has debit and credit cards. The person obtains customer rewards from grocery shopping, and a global positioning system (GPS) rests on the automobile's dashboard. On its face, this individual is reaping the rewards of a technological society [72].

In contrast, another individual lives in Camden, New Jersey, one of America's poorest cities. This person is underemployed while working part-time at a restaurant and being paid in cash. This individual survives in what is known as the underground economy. The person travels infrequently, does not have a passport, uses the Internet only at the local library, and pays cash when traveling by bus. Essentially, the lives of these two people are diametrically opposed to each other [73].

The contrast is stark. Big Data caters to the Manhattan resident and completely ignores the Camden resident as if that person did not exist. The Camden resident is alienated from society, and it is not unreasonable to suggest that this individual may feel a level of hostility towards the haves of the world so that they are capable of anything. Celente eloquently stated when he observed that when a person has lost everything and has nothing left to lose, they lose it [74]. This is the Camden resident, a potential revolutionary.

Surveillance and Privacy Matters Surrounding Big Data

Now, suppose that the essay focuses on the Manhattan resident as described in the previous subsection. As was previously posited, this individual has all of the benefits of Big Data. That person's activities and whereabouts are being scooped up with every click of a mouse and every step taken in their technological world. According to Zuboff, this individual is a seemingly willing

participant in surveillance capitalism, where the architecture of Big Data shifts the focus from Big Brother to Big Other [75]. The crux of the Big Data paradigm is that as Big Data dutifully caters to a person's every whim and desire, the individual never becomes aware that their freedom to choose is ever so gradually being eroded. Zuboff discerned that with negligible resistance from law or society, the controlled hive of being connected assures a drone-like dependency by individuals while at the same time virtually guaranteeing maximum profits at the cost of democracy and freedom [76].

In 2013, Snowden stunned the globe when he revealed that the American intelligence establishment was secretly collecting, storing, using, and disseminating every single phone call, text message, and email [77]. The result was that the federal government was shown to be the 800-pound Big Data gorilla in the room with the technical ability to peer into the lives of every person on the planet. Whether one agrees or disagrees with Snowden's disclosures, the fact that he demonstrated the level of detailed data that can be collected, stored, used, and disseminated shows not only the benefits of Big Data but also the costs to individual privacy.

Advertising and Marketing of Big Data

Advertising and marketing are essential to assuring the continued success of a business. According to Berkowitz et al., marketing is "the process of planning and executing the conception, pricing, promotion, and distribution of idea, goods, and services to create exchanges that satisfy individual and organizational objectives [78]." Marketing is not the same thing as advertising or personal selling because it is a far broader activity. In contrast, Skinner defined advertising to be a "paid form of communication about an organization, its products, or its activities that is transmitted through a mass medium to a target audience." Advertising provides marketeers, individuals engaged in marketing, the flexibility to communicate with a vast target audience [79] or concentrate on a small, precisely defined population segment. Advertising is a cost-effective promotional way because it can influence many people with a low cost per individual [80].

In many ways, marketing is a mechanism for achieving a competitive advantage [81]. With Big Data and other forms of e-commerce, the media of communication between a buyer and a seller is the Internet. Big Data not only collects substantial amounts of information about specific individuals, but it also gathers data about billions of people who detrimentally rely on the Internet at any time for their livelihood [82]. Thus, Big Data is an increasingly complex form of e-commerce, where e-commerce, or electronic commerce, is "the use of the Internet and the Web to transact business[83]." In Big Data and e-commerce, the focus is on digitally-empowered transactions between individuals and organizations. The transaction is usually commercial, typically involving an exchange of money for specified products and services. e-Business is different from e-commerce in that e-business is primarily concerned with "the digital enabling of transactions and processes *within* a firm, involving information systems under the control of the firm [84]." In many instances, e-business does not involve commercial transactions where an exchange of value occurs. For example, a firm's online inventory control mechanism is a form of e-business that does not generate revenue from outside customers. However, e-business supports e-commerce by providing the infrastructure where commercial transactions may happen [85].

Many Big Data companies, such as Amazon, eBay, or Yahoo!, are Internet storefront organizations, where an e-commerce storefront is an online vehicle that "combines transaction processing, security, online payment, and information storage to enable merchants [Big Data] to sell their products online [86]." A significant problem facing Big Data is how to attract volumes of people to come to a firm's website. This is a classic advertising and marketing issue because it is common knowledge that viewing an advertisement or a website does not guarantee that a person will accept the invitation to purchase Big Data's goods and services.

Traditionally, marketers employed loss-leaders to attract customers. According to Berkowitz et al., a

loss-leader is a product or service sold below market price to encourage buyers to purchase other goods at market price [87]. In a traditional business, loss-leaders are tangible products or services that a customer can experience at the transaction time. However, with Big Data and e-commerce transactions, there is a delay between the time that the transaction takes place and the time that the customer receives the benefits of the transaction. This delay is frequently because the shipment of the product or delivery of the service may take a few days, or even a week or more. This delay precipitates the customer experiencing buyer remorse, where buyer remorse is a "feeling of regret (= a wish that [one] had not done something) after making a choice or decision [88]." The timing delay may also increase buyer turnover and decrease purchasing frequency, where buyer turnover is "how often new buyers enter the market to by the product [or service] [89]" and where purchasing frequency is "the frequency of purchase of a specific product [or other products from the same vendor [90]."

Thus, to decrease buyer remorse and increase purchasing frequency, Big Data and other e-commerce businesses devised an extreme loss-leader – give away something of value for free – with the assumption that customers will be less inclined to make purchases elsewhere if they feel that they owe the company something in exchange for the free good or service, thereby making the transaction, at least in the mind of a customer, a bargained-for exchange. For companies like Google or Yahoo!, this means giving customers free email [91]. Although McDowell and Householder enumerated the benefits of free email are accessibility, competitive features, and additional capabilities [92], while its risks are security, privacy, and reliability, one issue that is conspicuous by its absence is who owns the emails that are sent and received by an individual.

According to the majority opinion in *Carpenter*, a cell phone owner has a reasonable expectation of privacy regarding cell phone metadata [93]. However, in this case, there were four separate dissents. The dissents by Justices Alito, Kennedy, and Thomas essentially argued that without property rights, there is no privacy [94]. However, Justice Gorsuch took a completely different approach in his dissent. He argued that the cell phone providers are bailees and the cell phone owners are bailors [95]. In other words, Justice Gorsuch opined that the property rights to cell phone metadata belong to the cell phone owners and not the cell phone providers.

Although not law, Justice Gorsuch's dissent is critical when deciding whether it should be legal for a firm that offers free email services (loss-leaders) to scan customer emails to discover relevant topics for advertisers. In some sense, emails are similar to cell phone metadata because customers probably have a reasonable expectation of privacy regarding their emails, but they may not have property rights. According to Lessig, the common law holds that privacy comes with property rights, consistent with the dissents of Justices Alito, Kennedy, and Thomas [96].

Thus, the answer to the question is that it is currently legal for email providers to scan an individual's email to find relevant topics for advertisers, provided that the email providers first obtain the consent of email customers. Even so, Justice Gorsuch's argument has merit. At some future date, if the Supreme Court uses Justice Gorsuch's dissent as the basis for future privacy decisions, it may turn out that the scanning activities of email providers will become illegal. Time will tell.

Contract Law and Big Data

Contract law is a complex legal field, so only the essentials will be discussed in this essay. A contract is a promise that the law will enforce [97]. It consists of an offer, an acceptance, and consideration. An offer is an objective communication that demonstrates the willingness of the maker to enter into a bargain with another party. An acceptance is an unequivocal assent to the terms and conditions of an offer. Finally, consideration is a valuable benefit that is bargained for between the parties. The consideration can take the form of money, promises, or actions. Consideration can be a bilateral exchange of benefits or unilateral action in exchange for a benefit[98]. The specific definitions of offer,

acceptance, and consideration depend on whether the common law or the Uniform Commercial Code is applicable.

There are various defenses to forming a contract, including misrepresentation, mistake, and statute of frauds. Misrepresentation occurs when one party intentionally, negligently, or innocently misrepresents the facts of the situation while the other party relies on this misrepresentation. A mistake happens when one or both parties believe a basic false assumption regarding the facts of the contractual situation. The statute of frauds is a customary law that specifies the conditions of when a contract should be in writing, including real estate agreements, contracts that take more than a year to be performed, suretyship agreements, marriage agreements, and the sale of tangible goods valued over $500 [99].

Under certain conditions, a contract can be modified by the parties or by the court. Conditions and the order of performance give meaning and effect to a contract. Conditions may specify when a promise is performed, either before or after the promise is executed. Parties may make warranties to the other party, where the warranty is either expressed or implied. A breach is a repudiation of the terms and conditions of a contract and may occur before the other party performs [100]. When a breach occurs, the remedies depend on the circumstances. The usual remedy is money damages, putting the non-breaching in a position as if the contract had been performed. This is known as expectation damages. Other remedies include restitution and reliance, where nominal damages are possible but not punitive damages. Damages can be general or special, where general damages typically measure the value lost because of the breach, while special damages are related to the effect of a breach on the other party [101].

The details of contract law are complex, and it is beyond the scope of this essay to analyze its nuances. However, what can be said is that common sense guideline should be followed when engaging in contracts. According to Laurence, there are ten recommendations that parties should follow in making solid business agreements [102]. They include:

1. Make sure that the contract is in writing;
2. Keep the agreement simple to understand;
3. When agreeing, deal with the person who has the authority to contract;
4. Correctly identify each party in the contract;
5. State specifically all of the details of the bargain;
6. Stipulate the payment obligations for all parties;
7. Agree on the circumstance where the contract may be terminated;
8. Decide on a way or method to resolve disputes;
9. Select the state law that will govern the contract; and
10. Keep the contract confidential [103].

These fundamental principles should be followed to ensure that a contract is performed successfully by all parties. It is a roadmap to ensure that contractual issues are kept to a minimum. It is the hidden agenda that all parties, including attorneys, should be cognizant of when making contracts.

Specific Contractual Recommendations

There are many legal issues that counsel should tackle when a cyber contract is negotiated [104]. An organization should try to understand what occurs when an existing security solution fails. Probably the most important issue that needs to be reexamined is the vendor selection process, particularly which individual in a company selects a supplier, what criteria were used to choose that supplier, and if the supplier's security process was considered during the selection process assuming that it existed. The company should perform an independent risk analysis of a supplier's security process, where counsel proactively advises the firm to pick vendors that comply with government and industry security regulations. In a Request for Proposal (RFP) process, an entity should get security commitments from its vendors during contract negotiations [105].

Counsel should demand that proper security requirements be included in supplier contracts. Counsel

should propose that existing contracts be evaluated and possibly renegotiated if possible. The SolarWinds attack showed that contractually obliging vendors to take appropriate precautions is insufficient[106]. A firm should validate the security posture of a supplier using independent reviews and audits if feasible. Counsel should petition that audit rights be contained in contracts and the notification of a security breach [107].

Counsel should warn their clients to remove their names from customer lists. This act alone will deter threat actors from capturing what suppliers a firm uses [108]. Counsel should call attention to that all-in-one solutions may imply that threat actors can use a single point of entry in trying to gain control over a system. A well-managed and diversified set of information technology (IT) tools decreases the risk of unauthorized access[109]. It should be understood that users want faster, more integrated technology with more functionality because, in IT, performance is critical. High-performance solutions increase the complexity of multifaceted systems and thus make them more challenging to secure. Counsel should work together with an IT department to (1) analyze the risks affiliated with complex software tools, (2) promote cybersecurity training for all employees, and (3) demonstrate the adverse effects of a breach[110].

The firm should appraise all user application privileges to ensure that users possess the least required privileges to perform their job. Applications with administrative access can mechanically act as a proxy for a user, system, or application. This is how the SolarWinds hack occurred. Counsel should encourage and contribute to periodic privilege reviews [111]. Finally, counsel should confirm that an entity has sufficient policies and resources to respond to a breach rapidly. Counsel should be acquainted with breach-notification, privacy laws, and third-party incident response organizations [112].

Summary of the Literature Review

This literature review discussed the definition of Big Data and the relevant federal and state statutes regarding the privacy that seemingly applies to Big Data. Other issues highlighted in the literature review included the Big Data paradoxes of transparency, identity, and power. An argument was made that, on its face, Big Data advocates transparency, identity, and power to the people, but the reality is just the opposite. Also, in this subsection, the essay observed that Big Data sings the melody of inclusion, but the song's words seem to indicate that individuals without Internet access are excluded from the chorus [113].

In the fourth subsection of the literature review, surveillance and privacy matters were described. Zuboff wryly noticed that as Big Data gathers more and more information about the personal preferences of its customers, the is a high likelihood that the personal choices will be dictated by Big Data and not decided independently by individuals. Furthermore, Snowden aptly pointed out that the federal government is likely the first instance of a Big Data organization because it has a myriad amount of data on its citizens [114].

Advertising and marketing were the following topics to be addressed in the literature review. The principles of advertising and marketing were explained. The question was asked whether it is legal for email providers to scan a person's email to unearth relevant subjects for commercial use. It was pointed out that given the current state of privacy in the United States, it is likely a legal activity, but that consent may be needed to overcome a reasonable expectation of privacy. Finally, the essentials of contract law were highlighted, and specific contractual were discussed in some detail. The tenor of the argument presented was that an attorney should pay particular attention to the contextual details to ensure that their clients are adequately protected.

Discussion of the Findings

The finding of the essay is manifold. First and foremost, Big Data seems to be a manifestation of a paradigm shift in information processing. Data are no longer conveniently structured in a linear fashion. Rather, semi-structured or unstructured data are dominating the information technology landscape. Big Data organizations are gathering and processing data from individuals at a breakneck pace to protect its citizens (governments) or

satisfy their customers (companies). The mantra of Big Data is apparently that this massive data collection is in everyone's best interest. However, the paradoxes of transparency, identity, and power seem to point in a different direction. According to Richards and King [115], Big Data is not the benevolent King (pun intended) advocated by Hobbes centuries ago [116]. In 1651, when this classic work was published, two short years had passed from 1649 when Charles I, then King of England, was beheaded for treason, and Oliver Cromwell ran the island nation for nearly ten years [117]. It was apparent from the literature review that power is being systematically concentrated in Big Data as more and more information about billions of people is collected, stored, used, and disseminated. There is a comparison between Big Data and a benevolent Hobbesian King who rules by divine right [118]. If history is repeated and usually does, then Big Data is in for a revolutionary surprise. If there is a comparison to be made, in the future, individuals may rebel against the intrusiveness of Big Data into their lives. Although it should be remembered that approximately ten after the beheading of Charles I, Cromwell died, and Charles II returned from exile to be crowned King of England, Ireland, and Scotland [119]. After Charles II died in 1685, scarcely a hundred years later, the American Revolution occurred, where the reason for the revolt was to defeat the tyranny of the Crown. Suppose Big Data follows this historical pattern in its search for freedom and autonomy from domination. In that case, the people may carve out yet another technology, a technology where freedom, transparency, and identity are cherished and upheld by law and as a positive technological outcome, and where power is truly in the hands of the people and not the mysterious Wizard King of Big Data.

Recommendations and Conclusion

The recommendations and conclusion of this essay are directed towards a single goal. Even though Big Data is now all the rage, Big Data should be dedicated to the propositions of transparency, identity, power to the people, and the inclusion of everyone, so that the benefits of Big Data are spread across the spectrum of individuals in the world. The threat of tyrannical Big Data is accurate, where the accumulation of information about the many may bring untold power that is held by the few. As Richards and King[120], and Leman[121], have eloquently observed, Big Data could potentially become the mechanistic master of humanity. Such a fate is anathema to the human psyche and soul. Hopefully, Richards, King, and Leman are wrong, but even so, time, as always, will be the final judge.

Miscellaneous Considerations

Author Contributions

The author has read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Conflicts of Interest

The author declares no conflicts of interest.

Acknowledgments

Not applicable.

Abbreviations

The following abbreviations are used in this manuscript

CCPA - California Consumer Privacy Act of 2018

CPA - Colorado Privacy Act of 2021

CPRA - California Privacy Rights Act of 2020

EEA - Economic Espionage Act of 1996

EGA - E-Government Act of 2002

EU - European Union

FISMA of 2002 - Federal Information Security Management Act of 2002

FISMA of 2014 - Federal Information Security Modernization Act of 2014

FMA - Financial Modernization Act of 1999

FTC - Federal Trade Commission

FTC Act - Federal Trade Commission Act of 1914

GDPR - General Data Protection Regulation

GLBA - Gramm-Leach-Bliley Act of 1999

GPS - Global Positioning System

HIPAA - Health Insurance Portability and Accountability Act of 1996

IT - Information Technology

MGTA - Modernizing Government Technology Act of 2018

NDAA - National Defense Authorization Act of 2017

OMB - Office of Management and Budget

RFP - Request for Proposal

SECURE IT - Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act of 2019

VCDPA - Virginia Consumer Data Protection Act of 2021

Highlights

1. Big Data is defined and described.
2. The relevant federal and state privacy laws are outlined, including the California Consumer Privacy Act as amended, the Virginia Consumer Data Protection Act, and the Colorado Privacy Act.
3. Several Federal Trade Commission privacy violation cases are highlighted.
4. The effects of Big Data collection and government surveillance are described.
5. Advertising and marketing are defined, where it is argued that while the scanning of emails by email providers may be legal, it should be accomplished with consent or not at all.
6. The essentials of contract law and specific contract negotiation techniques are outlined for the benefit of attorneys.
7. Finally, it is argued that although Big Data is the wave of the future, like all human institutions, it has in its definition the inherent paradoxes of transparency, identity, power, and exclusion that may potentially spell its undoing.

References

1. Alvin Toffler, The Third Wave (William Morrow & Company, Inc. 1980).
2. Oracle Staff, What is Big Data?, Oracle Inc. (n.d.), available at https://www.oracle.com/big-data/what-is-big-data/.
3. *Id.*
4. *Id.*
5. *Id.*
6. Viktor Mayer-Schönberger and Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work and Think (Mariner Books, 2014).
7. Nathan Marz, Big Data: Principles and Best Practices of Scalable Real-Time Data Systems (Manning Publications 2015).
8. Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-1839, available at https://www.congress.gov/104/plaws/publ294/PLAW-104publ294.pdf.
9. Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, available at https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.
10. Leighton Johnson, in Security Controls Evaluation, Testing, and Assessment Handbook (Academic Press 2nd ed. 2020), https://doi.org/10.1016/C2018-0-03706-8.
11. *Id.*
12. CDC Staff, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Centers for Disease Control and Prevention (Last reviewed Sep. 18, 2018), available at https://www.cdc.gov/phlp/publications/topic/hipaa.html.
13. *Id.*
14. Gramm-Leach-Bliley Act of 1999, Public Law 106-102,

available at https://www.govinfo.gov/content/pkg/PLAW-106publ102/html/PLAW-106publ102.htm.

15. Financial Modernization Act of 1999, Public Law 106-102, available at https://www.govinfo.gov/content/pkg/PLAW-106publ102/html/PLAW-106publ102.htm.
16. Gary Kranz, Gramm-Leach-Bliley Act (GLBA), TechTarget (Jun. 2021), available at https://searchcio.techtarget.com/definition/Gramm-Leach-Bliley-Act.
17. Federal Information Security Management Act of 2002, Public Law 107-347, available at https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf.
18. E-Government Act of 2002, Public Law 107-347, available at https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf.
19. NIST Staff, Federal Information Security Modernization Act (FISMA) Background, National Institute of Standards and Technology (Updated Sep. 28, 2021), available at https://csrc.nist.gov/projects/risk-management/fisma-background.
20. Federal Information Security Modernization Act of 2014, Public Law 113-283, available at https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.
21. *Id.*
22. *Id.*
23. Office of Management and Budget, Circular A-130, available at https://www.cio.gov/policies-and-priorities/circular-a-130/.
24. Modernizing Government Technology Act of 2018, H.R. 2227, available at https://www.congress.gov/bill/115th-congress/house-bill/2227.
25. National Defense Authorization Act of 2017, Public Law 114-328, available at https://www.govinfo.gov/content/pkg/PLAW-114publ328/html/PLAW-114publ328.htm.
26. Mick Mulvaney, Implementation of the Modernizing Government Technology Act, Office of Management and Budget (Feb. 27, 2018), available at http://www.whitehouse.gov/wp-content/uploads/2017/11/M-18-12.pdf.
27. *Id.*
28. Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act of 2019, Public Law 115-390, available at https://www.govinfo.gov/content/pkg/PLAW-115publ390/html/PLAW-115publ390.htm.
29. H.R.7327 - Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act, Congress.gov (Dec. 21, 2018) available at https://www.congress.gov/115/plaws/publ390/PLAW-115publ390.pdf.
30. Joseph Biden, Executive Order on America's Supply Chains, The White House (Feb. 24, 2021), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/.
31. *Id.*
32. *Id.*
33. General Data Protection Regulation, L119, 4 May 2016, p. 1-88, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL
34. Jake Frankenfield, revised by Amy Drury, General Data Protection Regulation (GDPR), Investopedia, (November 11, 2020), https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp; See also IT Governance Privacy Team, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide 11, 11 (2nd ed. 2017).
35. Id.
36. *Id.*
37. California Consumer Privacy Act of 2018, SB-375, available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

38. Donald L. Buresh, A Comparison between the European and American Approaches to Privacy, 6 Indonesian J. of Int. and Comp. L. 253, (2019), https://heinonline.org/HOL/LandingPage?handle=hein.journals/indjicl6&div=16&id=&page=.
39. *Id*.
40. *Id*.
41. California Privacy Rights Act of 2020, Prop. 24, available at https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf.
42. California Privacy Rights Act: An Overview, Privacy Rights Clearinghouse (December 10, 2020), https://privacyrights.org/resources/california-privacy-rights-act-overview#:~:text=The%20California%20Privacy%20Rights%20Act%20clarifies%20that%20people%20can%20opt,personal%20information%20to%20third%20parties.&text=The%20California%20Privacy%20Rights%20Act%20expands%20this%20to%20cover%20data,includes%20a%20username%20and%20password.
43. *Id*.
44. *Id*.
45. *Id*.
46. Virginia Consumer Data Protection Act of 2021, SB1392, available at https://legiscan.com/VA/text/SB1392/id/2328317.
47. Sarah Rippy, Virginia Passes the Consumer Data Protection Act, Int'l. ass'n. of Priv. Prof., (Mar. 3, 2021), https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/.
48. Colorado Privacy Act of 2021, SB21-190, available at https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_enr.pdf.
49. Sarah Rippy, Colorado Privacy Act Becomes Law, The Privacy Adviser (Jul. 8, 2021), https://iapp.org/news/a/colorado-privacy-act-becomes-law/.
50. Nevada Privacy Law, NRS 603A.300 – 603A.360 as amended by SB 220, available at https://www.leg.state.nv.us/nrs/nrs-603a.html.
51. An Act To Protect the Privacy of Online Customer Information, LD 946, available at https://www.mainelegislature.org/legis/bills/bills_129th/billtexts/SP027501.asp.
52. Donald L. Buresh, Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?, 38 Santa Clara High Tech. L. J. 1, 39-93 (Oct. 2021), https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2/.
53. In the Matter of TaxSlayer, LLC, FTC Matter/File No. 162 62 063, available at https://www.ftc.gov/enforcement/cases-proceedings/162-3063/taxslayer.
54. In the Matter of Everalbum Corp., FTC Matter/File No. 192 3172, available at https://www.ftc.gov/enforcement/cases-proceedings/192-3172/everalbum-inc-matter.
55. Isabella Jibilian, & Katie Canales, The US Is Readying Sanctions Against Russia Over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal, Business Insider (Apr. 15, 2021), available at https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.
56. In the Matter of TaxSlayer, LLC, Complaint Docket No. C-2646 (n.d.), available at https://www.ftc.gov/system/files/documents/cases/1623063_c4626_taxslayer_complaint.pdf.
57. *Id*.
58. In the Matter of Everalbum, Inc., United States of America before the Federal Trade Commission (May 7, 2021), available at https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_complaint.
59. See 15 U.S. Code § 45 (a)(1), Legal Information Institute, available at https://www.law.cornell.edu/uscode/text/15/45.
60. Andy Greenberg, Hacker Lexicon: What Is a Supply

Chain Attack?, Wired (May 31, 2021), available at https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/.

61. *Id*.
62. *Id*.
63. Neil M. Richards, & Jonathan H. King, Three Paradoxes of Big Data, 66 Stan. L. Rev. 41 (2013), available at https://www.stanfordlawreview.org/online/privacy-and-big-data-three-paradoxes-of-big-data/.
64. *Id*.
65. *Id*.
66. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harvard L. Rev. 193, 193 (1890).
67. Gattaca (Andrew Niccol dir. 1997).
68. Samuel D. Warren & Louis D. Brandeis, supra, note 45.
69. Mike Wallace, The Mike Wallace Interview: Aldous Huxley (1958-05-18), YouTube (May 18, 1958), available at https://www.youtube.com/watch?v=1ePNGa0m3XA. (Here, Aldous Huxley opined to Mike Wallace that in the future, people will be taught to love their slavery, and shall love their slavery).
70. Neil M. Richards, & Jonathan H. King, supra, note 42.
71. Jonas Leman, Big Data and Its Exclusions, 66 Stan. L. Rev. 55 (2013), available at https://www.stanfordlawreview.org/online/privacy-and-big-data-big-data-and-its-exclusions/.
72. *Id*.
73. *Id*.
74. Gerald Celente, Glen Beck's War Room, FoxNews (Feb. 23, 2009), available at https://www.foxnews.com/story/glenn-becks-war-room.
75. Shoshana Zuboff, The Age of Surveillance Capitalism (Public Affairs Press 2019).
76. *Id*.
77. Edward Snowden, Permanent Record (Metropolitan Books 2019).
78. Eric N. Berkowitz, Roger A. Kerin, Steven A. Hartley, & William Rudelius, Marketing 10 (Irwin Publishers 4th ed. 1994).
79. Steven J. Skinner, Marketing 587 (Houghton Mifflin Company 2nd ed. 1994).
80. *Id*.
81. Michael E. Porter, Competitive Advantage: Creating and Sustaining Superior Performance (The Free Press 1985).
82. Viktor Mayer-Schönberger and Kenneth Cukier, supra, note 6.
83. Kenneth C. Laudon, & Carol Guercio Traver, e-Commerce: Business Technology Society 10 (Pearson Publishing 4th ed. 2008).
84. *Id*. at 11.
85. *Id*.
86. H. M. Deitel, P. J. Deitel, & K. Steinbuhler, e-Business and e-Commerce for Managers 28 (Prentice-Hall Publishing 2001).
87. Eric N. Berkowitz, Roger A. Kerin, Steven A. Hartley, & William Rudelius, supra, note 57.
88. Buyer Remorse, Cambridge Dictionary (n.d.), available at https://dictionary.cambridge.org/us/dictionary/english/buyer-s-remorse.
89. Eric N. Berkowitz, Roger A. Kerin, Steven A. Hartley, & William Rudelius, supra, note 57 at 543.
90. *Id*. at 726.
91. See generally, Louis Alexander, Why Emails Are Free to Use?, Workspace (n.d.), available at https://workspace.digital/why-are-emails-free-to-use/.
92. Mindi McDowell, & Allen Householder, Security Tip (ST05-009): Benefits and Risks of Free Email Services, Cybersecurity & Infrastructure Security Agency (rev. Sep. 27, 2019), available at https://us-cert.cisa.gov/ncas/tips/ST05-009.
93. Carpenter v. United States, 585 U.S. ___ (2018).
94. *Id*.
95. Donald L. Buresh, The Meaning of Justice Gorsuch's Dissent in Carpenter v. United States, 43 Amer. J. of Trial Advocacy 1 55-103 (2019), available at https://

heinonline.org/HOL/LandingPage?handle=hein.journals/amjtrad43&div=7&id=&page=.

96. Lawrence Lessig, Privacy as Property, 69 Social Research 1 (2002), available at https://www.jstor.org/stable/40971547?seq=1#page_scan_tab_contents.

97. Jeffrey Ferriell, & Michael Navin, Understanding Contracts (LexisNexis Publishing 2004).

98. *Id*.

99. *Id*.

100. *Id*.

101. *Id*.

102. Bethany K. Laurence, Ten Tips for Making Solid Business Agreements and Contracts, Nolo (n.d.,), available at https://www.nolo.com/legal-encyclopedia/make-business-contract-agreement-30313.html.

103. *Id*.

104. Carina Mendola, & Brett Creasy, Lessons Learned from the SolarWinds Hack: What Went Wrong & How Can Lawyers Help Mitigate the Risk of Cyberattacks, Association of Corporate Counsel (n.d.), available at https://www.acc.com/sites/default/files/2021-02/Lessons%20Learned%20from%20the%20SolarWinds%20Hack.pdf.

105. *Id*.

106. Id.

107. Id.

108. Id.

109. *Id*.

110. *Id*.

111. *Id*.

112. *Id*.

113. Shoshana Zuboff, supra, note 54.

114. Snowden, supra, note 56.

115. Richards and King, supra, note 42.

116. Thomas Hobbes, Leviathan (Penguin Classics 2017).

117. See generally, History.com Editors, King Charles I Executed for Treason, History.com (Jul. 28, 2019), available at https://www.history.com/this-day-in-history/king-charles-i-executed-for-treason.

118. Hobbes, supra, note 95.

119. Biography.com Editors, Charles II of England, Biography.com (Oct. 6, 2021), available at https://www.biography.com/royalty/charles-ii-of-england.

120. Richards and King, supra, note 42.

121. Leman, supra, note 50.