CONVERGENCE OF FORENSICS, EDISCOVERY, SECURITY, & LAW

Serge Jorgensen[†]

INTRODUCTION

Moore's Law, an observation first made in 1965, predicts that the number of transistors on integrated circuits will double approximately every two years.[1] For technologists, an extension of this means that everything that relies on integrated circuits, from computer speeds to the resolution of digital cameras, will also double every couple of years.[2] For lawyers and consumers, this means that technology is not going to stop changing any time in the near future. Technological advances will bring new challenges and new considerations at an ever faster pace as data processing and storage reach into unforeseen areas of our lives. Agreements, or arguments, about native versus TIF formats of production pale in comparison to issues such as forensics and data discovery on neural networks,[3] "big data,"[4] or crowd-

[†] Serge Jorgensen is a founding partner in the Sylint Group, and provides technical development and guidance in the areas of computer security, counter cyber-warfare, system design, and incident response. Mr. Jorgensen holds various patents in engineering and math-related fields. Prior to co-founding the Sylint Group, Mr. Jorgensen ran the research and development department for Locast Corporation, developing a HIPAA-compliant patient location and status-tracking device. As part of this effort, Mr. Jorgensen developed proprietary secure, low-bandwith data transmission techniques and methodologies implementing secure communications technology. For end-user and collaborative users, Mr. Jorgensen designed and implemented secure software and data-storage models and tools to collect, transmit and store confidential patient information. Since co-founding the Sylint Group, Mr. Jorgensen has, among other things, directed development of DNA tracking applications; responded to multi-billion dollar international espionage and cyber-security attacks; and directed, tasked, and managed multi-million dollar litigation, forensic, and electronic discovery efforts. Mr. Jorgensen has held various security clearances and works closely with the FBI in tasking, analysis, and managing information security needs to safeguard critical infrastructure of U.S. manufacturing processes. Mr. Jorgensen develops, engineers and implements secure communication protocols, traffic analysis techniques, and malware identification and remediation efforts. Internationally, Mr. Jorgensen has provided briefings to King Juan Carlos of Spain and the Minister of Defense for Singapore.

[1] *Moore's Law*, WEBOPEDIA, http://www.webopedia.com/TERM/M/Moores_Law.html (last visited May 15, 2014).

[2] *Id.*

[3] Neural networks are "[a] type of artificial intelligence that attempts to imitate the way the brain works" by "creating connections between processing elements, the computer equivalent of

sourced solutions architected and adopted by companies including Facebook, Unilever and Netflix.[5] There are currently a staggering seven billion-plus cell phones for the 4.7 billion people between the ages of fifteen and sixty-four in the world.[6] The possibilities for connectivity and data creation created by this fact alone are staggering. Start adding other potential discovery sources, such as larger computers, digital cameras, automobile navigation systems and the Internet of Things (IoT),[7] and there is a mess of data. Trying to adequately secure, acquire, examine and produce related data, let alone determine legal relevance, is becoming an increasingly daunting task. The proposition that one can still "look through the filing cabinet" for legally relevant electronically stored information (ESI) or discoverable data is simply untrue. We now need to know what to keep, where to keep it, and how to look for it when the need arises—and in order to have a chance of finding what we are looking for, we need to know these things *before* we know we need the data.

As society develops and incorporates new technologies, it will become obvious that the law must move to a more proactive stance, instead of the current reactive stance. The challenges of ESI Forensics, Discovery, and Security in the distributed, scalable, shared computing infrastructure commonly called "the cloud" are in a large part a result of our prior failings to proactively consider compliance and legal matters *before* adopting these new technologies. This is not an argument for new laws, but rather to apply

neurons," rather than basing all decisions on manipulating ones and zeroes. *Neural Network*, WEBOPEDIA, http://www.webopedia.com/TERM/N/neural_network.html (last visited May 19, 2014) (emphasis omitted).

[4] Big data describes a large volume of data that is too large to easily process using traditional data processing techniques. *Big Data*, WEBOPEDIA, http://www.webopedia.com/TERM/B/big_data.html (last visited May 19, 2014).

[5] Crowdsourcing's purpose is to take advantage of the collective intelligence of the public to complete business-related tasks, enabling companies to take advantage of a wider talent pool while also gaining further insight. Jennifer Alsever, *What Is Crowdsourcing?*, CBSNEWS (May 1, 2008, 5:41 PM), http://www.cbsnews.com/news/what-is-crowdsourcing/. For a list of companies engaging in crowdsourcing projects, see *List of Crowdsourcing Projects*, WIKIPEDIA, http://en.wikipedia.org/wiki/List_of_crowdsourcing_projects (last visited May 12, 2014).

[6] *International Data Base*, U.S. CENSUS BUREAU, http://www.census.gov/population/international/data/idb/region.php?N=%20Results%20&T=15&A=aggregate&RT=0&Y=2014&R=1&C= (last visited May 15, 2014) (search of U.S. Census Bureau's international population database searching for entire world's population in 2014, broken down by broad age range groups, results aggregated); Joshua Pramis, *Number of Mobile Phones to Exceed World Population by 2014*, DIGITAL TRENDS (Feb. 28, 2013), http://www.digitaltrends.com/mobile/mobile-phone-world-population-2014/.

[7] The Internet of Things (IoT) refers to the idea of connecting physical objects to other objects, allowing them to communicate, greatly increasing their ability to track information about the user and about the devices themselves. *Internet of Things (IoT)*, TECHOPEDIA, http://www.techopedia.com/definition/28247/internet-of-things-iot (last visited May 19, 2014).

existing laws and current solutions to these new technologies. We otherwise risk tossing aside years of experience and knowledge. Current statutory and common law legal authority is well equipped to deal with many, perhaps even all, legal questions that might arise from the use of new technology. In most cases, a clear similarity can be found between the physical world of houses, floors, walls, doors, and windows and the logical world of networks, infrastructure, routers, firewalls, and packets. Privacy, ownership, access, control, responsibility—all of these concepts and many more exist in both physical and logical worlds.

The following discussion will provide some basic definitions of various terms and components, review tools and resources available, and offer a glimpse of upcoming technological advances and the associated convergence between legal and technical considerations as those technologies develop.

This Article is not meant to provide exhaustive descriptions of each area, but will cover some foundational concepts and suggest a path where lawyers and technologists can coexist in a symbiotic, instead of an antagonistic, relationship. Lawyers are generally risk-averse, and (at least to technologists) have gained a reputation over the years as impediments to progress and innovation. First-adopters of available technologies (inventors, entrepreneurs, and the like) are less risk-averse, or even risk-seeking, and generally leap before looking. This risk-oriented culture has been responsible for creating new and innovative ways to collect and share information. Without anticipating and building in some forethought protections, such innovations pose currently-unaddressed and techno-centric legal issues that affect each of our lives to an increasingly insidious extent.

I. DEFINITIONS

An effective discussion on the subject of convergence must first clear up confusion regarding some terms and usages common in the industry. Technologists and attorneys frequently get themselves into trouble by using presumed (and at times incorrect) definitions of terms that mean different things to each group. For the purposes of our discussion, the reader is asked to generally accept the following descriptions of forensics, electronic discovery and information security. These are not meant to be complete, nearly-complete, or even permanent definitions, but rather, foundational overviews that will provide the groundwork for a further discussion on some areas of convergence between these areas and the legal world. While it would be easy to argue that the offered definitions are overly simplistic and cover but a fraction of the areas of expertise involved in each, the alternative would be to write a series of books on each subject by itself.

A. *Forensics*

"Computer forensics" is a term commonly used to describe the in-depth analysis of ESI.[8] Even that definition, however, is open for interpretation and can result in confusion. Consider "the computer." This is generally understood to mean a collection of components made up of a processor, some volatile memory (RAM), some non-volatile memory (hard disk drives or HDD), a keyboard, screen, mouse, power supply, DVD drive, and various other parts.[9] While one could expect that the data on the HDD is the key component, a forensic analyst might also consider:

- the Service Tag on the case of the computer to determine if the HDD is the original equipment;
- SMART information to evaluate power-on cycles and other internal information; and even
- the placement of dust inside the case to assess other physical access to the system.

Similarly, when scrutinizing data on an HDD, a forensic expert knows that there is data in allocated space, unallocated space, slack space and manufacturer-controlled spaces and data repositories.[10] Moreover, chain of custody, best-evidence and provenance are all forensic considerations when examining a potential source of information.

For the purposes of this discussion, forensic analysis of "the computer" generally includes review of some sort of data repository (e.g., a HDD) and

[8] Susan Steen & Johnette Hassell, *Computer Forensics 101*, EXPERTLAW (Oct. 2004), http://www.expertlaw.com/library/forensic_evidence/computer_forensics_101.html.

[9] *Parts of a Computer*, WINDOWS, http://windows.microsoft.com/en-us/windows/computer-parts#1TC=windows-7 (last visited May 12, 2014).

[10] These terms describe different areas on a hard drive. Unallocated space is the area on the hard drive that is available for the computer to write data to, including any blank space on a hard drive or space where a file has been deleted. *What Is the Difference Between Unallocated Space and Active or Allocated Space*, CENTER FOR COMPUTER FORENSICS, http://www.computer-forensics.net/FAQs/what-is-the-difference-between-unallocated-space-and-active-or-allocated-space.html (last visited May 19, 2014). This space requires computer forensic software to view and analyze. *Id.* Allocated space is the area on the hard drive that contains the operating system and files that a computer user can access. *Id.* Slack space refers to the space on a hard drive between the end of a file and the end of the disk cluster it is stored in, which results because data rarely fills fixed storage locations exactly. *Definition of: Slack Space*, PCMAG.COM, http://www.pcmag.com/encyclopedia/term/56995/slack-space (last visited May 19, 2014).

the information placed on that HDD by an operating system (OS). Difficulties can arise when evidence moves from the physical to the virtual world—or from local to the remote locations. In years past, "the computer" contained one or two HDDs and was located under someone's desk. It is increasingly common for computers to contain multiple drives with terabytes of storage and to be located in some location or locations remote from the user. Virtualization technology makes it possible, and even likely, that one physical HDD contains many more than one virtual environment (OS and user experience). Cloud technology and cheap high-speed internet access make it probable that there is more data stored in a remote location (e.g., SkyDrive, iCloud, GoogleDocs) than on the local computer.[11] Any forensic analysis that fails to at least consider these other data repositories is both inadequate and incomplete, and testimony based on such analyses is susceptible to easy impeachment.

Two major components of a forensic investigation are the *Preservation* and the *Analysis* of data.[12] In order to discuss data preservation, it is necessary to fully understand the process of the creation and usage of the data. Once the forensic analyst understands this data creation and usage, the appropriate techniques can be brought to bear on the various data repositories. Live, offline, virtual, remote, and snapshot acquisitions each have their place and value, and each have their advantages and disadvantages. Depending on the data and environment, partial preservation may be the "best efforts"[13] of a party and work will need to be done on a live system. This is most often the case in mobile devices (i.e., smartphones) where full forensic acquisition is often impossible due to manufacturer constraints on access to the raw data repositories on the devices. A brief convergence discussion will aid in understanding the need for counsel to appreciate the complexities and limitations of the various collection and preservation options. Failure to take the time to adequately

[11] SkyDrive, iCloud, and GoogleDocs are examples of data repositories held on shared storage in an offsite location or, in common parlance, a "personal cloud." *Personal Cloud*, GARTNER, http://www.gartner.com/it-glossary/personal-cloud (last visited May 12, 2014). *See also Microsoft OneDrive*, ONEDRIVE, https://onedrive.live.com/about/en-us (last visited May 12, 2014) (describing services provided by OneDrive); *What Is iCloud?*, ICLOUD HELP, http://help.apple.com/icloud/ (last visited May 12, 2014) (describing services provided by iCloud); *Docs, Sheets, and Slides*, GOOGLE, https://support.google.com/docs/answer/49008?rd=1 (last visited May 12, 2014) (describing services provided by Google Docs).

[12] Marcus K. Rogers et al., *Computer Forensics Field Triage Process Model*, 1 J. DIGITAL FORENSICS, SECURITY & L., no. 2, 2006, at 19, 21 fig.1.

[13] E. Jane Sidnell & Christopher P. Knight, *"Best Efforts"—"Reasonable Efforts"—"Commercially Reasonable Efforts"—What Do These Terms Mean?*, LEXOLOGY (June 7, 2010), http://www.lexology.com/library/detail.aspx?g=6a4c20dc-594d-4756-b710-7a2dc213e8c0.

understand the methods and limitations will easily result in widely differing definitions of the words “everything” and “all” with the near certainty of an associated negative outcome. Promising or agreeing to preserve “everything” without careful research and a clear understanding of capabilities and options can be disastrous.

Once preservation has occurred, or access methodologies have been agreed upon, the analysis can commence. Analysis, from the earlier example, can include both physical and logical work and spans a wide range of skills. Once past a cursory inspection, analysis of the logical environment generally consists of collecting and reviewing surrounding information as much as the data in question. Translating this into the physical world, a CSI agent would spend as much time examining the space *around* the dead body as on the dead body itself. Likewise, a good computer forensic analyst will develop information about the system metadata,[14] computer usage patterns, registry information[15] and various other indicators before focusing on the specific data that might be the “focus” of the analysis.

For a short review of a forensic analyst’s work, consider as an example a simple Microsoft Word document created in a Windows operating system and saved on a local hard drive. Taken together, the information contained would include the various components shown in Figure 1.

[14] “Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about data or information about information.” NAT’L INFO. STANDARDS ASS’N, UNDERSTANDING METADATA 1 (2004), *available at* http://www.niso.org/publications/press/UnderstandingMetadata.pdf.

[15] A registry is a database used by the operating system, such as Windows, to store configuration information about the software on a computer, such as the desktop background and program settings. *Registry*, TECHTERMS.COM, http://www.techterms.com/definition/registry (last visited May 19, 2014).

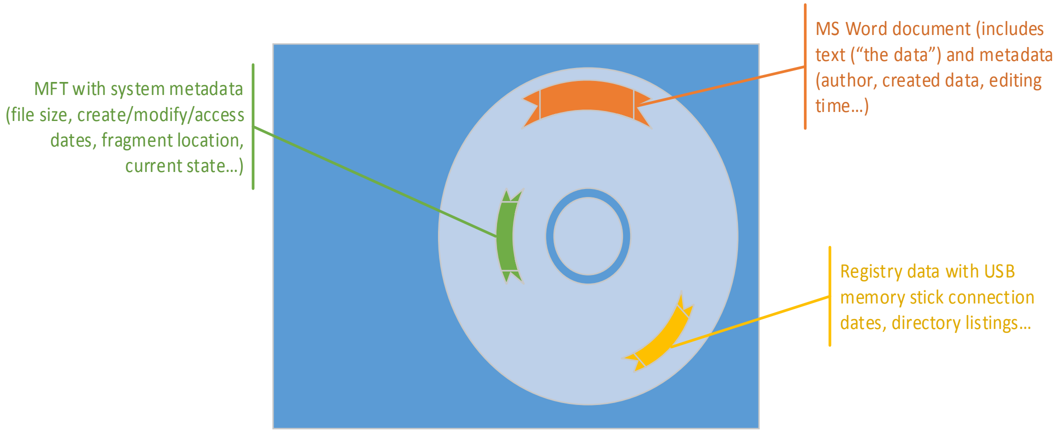

MS Word document (includes text ("the data") and metadata (author, created data, editing time…)
MFT with system metadata (file size, create/modify/access dates, fragment location, current state…)
Registry data with USB memory stick connection dates, directory listings…

Figure 1

As briefly described in the associated blocks, certain sectors of the HDD will contain the actual words in that document as well as some basic information captured by the program that created those words. Other sectors, however, contain potentially much more interesting (and likely relevant) bits of data that can tell a story about what happened to the document—such as when it was created (or deleted) as recorded by the Master File Table (MFT),[16] where it might have come from or gone to, and what other documents or files might be associated with it. This relevant data is scattered through various places in, using Windows parlance as an example, the registry, MFT, etc. Like our CSI agent, the skilled forensic investigator begins to recreate not just the murder victim, but the entire scene of the crime. Not surprisingly, like a *clumsy* CSI agent can contaminate a scene with footprints and foreign debris, a careless interloper (or a curious IT person or lawyer) can easily and irreversibly alter or destroy critical evidentiary material.

[16] The MFT performs a similar function for a Windows-based operating system as a table of contents does to a book; it tracks the location of each file and folder on the HDD and some basic information about the file or folder. *Master File Table*, MICROSOFT DEVELOPER NETWORK, http://msdn.microsoft.com/en-us/library/windows/desktop/aa365230(v=vs.85).aspx (last visited May 12, 2014); *How Windows Stores Files and How Defraggler Works*, PIRIFORM, http://www.piriform.com/docs/defraggler/technical-information/how-windows-stores-files-and-how-defraggler-works (last visited May 15, 2014).

B. *Electronic Discovery*

Discovery related to digital evidence, more commonly known as ESI, is commonly referred to as electronic discovery, or eDiscovery.[17] Discussions about eDiscovery typically revolve around:

- data repositories, or where is data kept;[18]
- data custodians, or who owns or controls the data;[19]
- metadata, or data about the data;[20]
- search processes, terms and techniques; and
- production format.

Looking at these areas, hopefully the reader can begin to see some convergence between the forensic role of preservation of data repositories and metadata from chosen data custodians and the eDiscovery role of the extraction, production, and evaluation of relevant data from the identified data repositories, metadata, and custodians. Incomplete or partial understanding of data identification and preservation techniques can severely limit the data available for an electronic discovery exercise. Likewise, not understanding the necessary scope of the discovery efforts can easily result in needless, or improperly focused, forensic efforts.

Once evidence has been properly preserved from alteration, discovery efforts can commence. Techniques vary widely, but, fancy terminology notwithstanding, generally include some means of computerized sifting through data for some pre-defined collection of words. Using an example of searching for a document concerning motorcycles, the techniques shown in Table 1 would have various degrees of computer support. Linguistic analysis of the desired subjects can be recursively combined to give potentially more and more accurate results.

Technique	**Search Terms**
Keyword	Motorcycle
Fuzzy Keyword	motorcycle, motercycle, motorcycel, motorcycling

[17] THE SEDONA CONFERENCE GLOSSARY: E-DISCOVERY & DIGITAL INFORMATION MANAGEMENT 16 (Sherry B. Harris & Paul H. McVoy eds., 4th ed. 2014).

[18] *Data Repository*, TECHOPEDIA, http://www.techopedia.com/definition/23341/data-repository (last visited May 19, 2014).

[19] *Data Custodian*, WEBOPEDIA, http://www.webopedia.com/TERM/D/data_custodian.html (last visited May 19, 2014).

[20] NAT'L INFO. STANDARDS ASS'N, *supra* note 14, at 1.

Context	motorcycle, bike, harley, hog, scooter

Table 1

How these keywords and contexts are derived is a combination of art and science. In some of the more advanced concepts of predictive coding[21] and Technology Assisted Review (TAR), collections of keywords are self-generated and ranked by the computer after the searcher assigns certain amounts of relevance to various documents.[22] Search methods routinely become part of legal arguments regarding efficacy, and parties assert that searches are either overbroad or inaccurate as it suits their case.[23]

As globalization increases, the difficulties of language nuances are also becoming more apparent in searches. Just like the U.S.-famous movie *Grease* was renamed to *Brillantina* in South America because of translation issues,[24] using our earlier example, terms and concepts for "motorcycle" may vary widely when moved across languages and contexts. Thus, using a non-native speaker (or Google Translate) can create significant holes in any cross-language searches.[25] Though this is not an area where the law needs to be ahead of technology, it represents another area in which those that practice law must stay abreast of technology and technological advances.

Just like foreign languages, and similar to the forensic and preservation issues described earlier, technological terms can, and often do, create confusion during the eDiscovery process. Lawyers (and courts) that try to provide every possible example when defining ESI may quickly find their documents outdated the moment they are sent, so they, instead, should adopt

[21] Predictive coding uses keyword search, filtering and sampling to automate parts of an e-discovery document review in order to reduce the number of irrelevant and non-responsive documents that need to be reviewed manually. Margaret Rouse, *Predictive Coding*, SearchCompliance (Aug. 31, 2012), http://searchcompliance.techtarget.com/definition/predictive-coding. Judicial attitudes toward predictive coding have begun to change recently, as judges have become more accepting of it. Akiva M. Cohen, *The Defensibility Question*, it-lex (Apr. 10, 2013), http://it-lex.org/evolving-judicial-attitudes-towards-predictive-coding-suggest-it-may-soon-be-time-to-retire-the-defensibility-question/.

[22] *The Grossman-Cormack Glossary of Technology-Assisted Review*, EDRM, http://www.edrm.net/resources/glossaries/grossman-cormack (last visited May 12, 2014).

[23] *See* Da Silva Moore v. Publicis Groupe, 287 F.R.D. 182, 191 (S.D.N.Y. 2012) (criticizing keyword searchers as being both over-inclusive and under-inclusive, because they return a large number of irrelevant documents while also excluding many relevant documents).

[24] *Grease (1978) Trivia*, IMDB, http://www.imdb.com/title/tt0077631/trivia (last visited May 12, 2014). This title translates as "hair oil." *Brillantina*, WordReference.com, http://www.wordreference.com/es/en/translation.asp?spen=brillantina (last visited May 16, 2014).

[25] For an example of the limitations of the limitations of Google Translate, see Jenny Ann, *How Accurate Is Google Translate, Really?* (Apr. 27, 2013), http://www.digitaltrends.com/web/how-accurate-is-google-translate/#!OWpsS (describing differences in text after translating it from English into other languages and then back to English).

sufficiently broad standards.[26] Producing parties that fail to take context into consideration when deciding where to search often raise questions of completeness and find themselves forced to re-do their efforts.[27]

The next issue that arises in eDiscovery cases relates to forms of discovery production. These vary from printed copies of emails to native format of databases, and seem to directly relate to the interest of the producing party in resolving technical issues and addressing the questions of law. Here, a strong Federal Rule 26(f) conference,[28] regardless of requirements, can go a long way towards resolving misunderstandings, reducing costs, and allowing parties to focus on arguments of law instead of arguments of data.[29] There are many good reasons why different formats of production may be necessary and valuable, and it is only through conversation between parties and a clear understanding of the technology at play that the proper format and solution can be determined.

C. *Information Security*

Finally, information security's role is to allow, deny, and track access to various data repositories. Passwords, logs, and traffic flow all become part of the security world. Staying with the convergence concept, if forensics is the preservation and analysis of data repositories and metadata from chosen

[26] For an example of such a protocol, see Suggested Protocol for Discovery of Electronically Stored Information (D. Md.), *available at* http://www.mdd.uscourts.gov/news/news/esiprotocol.pdf.

[27] For example, in *In re Fannie Mae Securities Litigation*, third party OFHEO was ordered to produce records it collected in preparing an investigation report. *In re* Fannie Mae Sec. Litig., 552, F.3d 814, 816 (D.C. Cir. 2009). OFHEO sought to limit its production by asking parties to limit their requests for electronically stored information, to which the defendants agreed. *Id.* After OFHEO stated that it had produced all requested documents, it was discovered that OFHEO had failed to search all of its off-site disaster-recovery backup tapes, leading to a motion for sanctions against OFHEO for failing to produce all requested documents. *Id.* at 817. OFHEO and the defendants agreed to a stipulated order holding the contempt order in abeyance and requiring OFHEO to search its disaster-recovery backup tapes and provide all responsive documents to the defendants. *Id.* Notably, the defendants were to specify the search terms to be used. *Id.* The defendants wound up submitting over 400 search terms, covering 600,000 documents. *Id.* Despite seeking to comply with the search terms, OFHEO was unable to meet the deadline and the court imposed sanctions forcing the production of all documents for which OFHEO claimed privilege to defendants' counsel for review, noting OFHEO's repeated failure to meet deadlines. *Id.* at 818.

[28] Parties are generally required to hold such a conference to "consider the nature and basis of their claims and defenses and the possibilities for a prompt settlement or resolution of the case, to make or arrange for the disclosures required by Rule 26(a)(1), to discuss any issues relating to preserving discoverable information, and to develop a proposed discovery plan. . . ." FED. R. CIV. P. 26(f).

[29] THE SEDONA CONFERENCE COOPERATION PROCLAMATION: RESOURCES FOR THE JUDICIARY 13 (Ronald J. Hedges & Kenneth J. Withers eds., 2011), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/SedonaRes.pdf/$file/SedonaRes.pdf.

data custodians, and eDiscovery is the extraction, production and evaluation of relevant data from the identified data repositories, metadata, and custodians, it follows that information security is the gatekeeper that logs access to and from the data repositories, creates much of the metadata surrounding the data, and identifies the custodians involved.

Thus, Information Security policy and processes are thus inextricably interwoven into any eDiscovery or Forensics activity. Concerns may arise when Security is seen as an access *preventer* (e.g., "*I* can't access my data") instead of an access *controller* (e.g., "No one else *but* me can access my data"). In the attempt to make user access as seamless as possible, there have been frequent lapses which result in open access (e.g., "Yikes! *Everyone* can access my data") whether through password compromises[30] or code errors.[31]

Concepts of data security are generally tied to data usage or data ownership. The "rights" to access something are based on pre-defined criteria which, like the law, is facing a greater and greater challenge. The concept of user rights to data, and the associated granting or revocation of those rights, must grow more flexible as data is created, aggregated, and analyzed in greater quantities and in a more fluid fashion. Various Terms of Service (ToS)[32] and Service Level Agreements (SLAs)[33] suggest a set of assumed (or taken) rights and privileges assigned to the company providing the compute platform. In recent updates to Privacy Policies, Microsoft[34] and Google[35] have both affirmed their belief to their right to look through any

[30] One example of this is Yahoo!, who suffered an attack where a hacker was able to access a list of usernames and passwords, giving the hacker access to Yahoo! Mail accounts. Chris Smith, *Hack Alert: Change Your Yahoo Mail Password Right Now*, YAHOO NEWS (Jan. 31, 2014, 8:35 AM), http://news.yahoo.com/hack-alert-change-yahoo-mail-password-now-133533509.html.

[31] This happened to Dropbox, where a bug in its authentication system allowed some users to log in without using the correct password. John E. Dunn, *Dropbox Admits It Suffered Serious Password Failure*, CSO ONLINE (June 21, 2011, 8:00 AM), http://www.csoonline.com/article/684849/dropbox-admits-it-suffered-serious-password-failure.

[32] A ToS lays out the rules the user of a service must follow to use the service. *Definition of: Terms of Service*, PC MAG., http://www.pcmag.com/encyclopedia/term/62682/terms-of-service (last visited May 15, 2014). *See also Terms of Service Didn't Read*, TERMS OF SERVICE; DIDN'T READ, http://tosdr.org (last visited May 12, 2014) (summaries of various ToS agreements).

[33] SLAs define the expected quality of services that users can expect to receive. Lynn Greiner & Lauren Gibbons Paul, *SLA Definitions and Solutions*, CIO, http://www.cio.com/article/128900/SLA_Definitions_and_Solutions (last visited May 12, 2014).

[34] *See Microsoft Online Privacy Statement*, MICROSOFT (Aug. 2013), http://privacy.microsoft.com/en-us/fullnotice.mspx#EIC. *See also* Christina Warren, *Microsoft Tracks Down Rogue Employee by Snooping Blogger's Hotmail*, MASHABLE (Mar. 20, 2014), http://mashable.com/2014/03/20/microsoft-email-access-blogger/.

[35] *See In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 U.S. Dist. LEXIS 172784 at *26 (N.D. Cal. Sept. 26, 2013) ("Google argues that its reading of any emails would fall within the

information hosted on their systems. For MS365 and Gmail users, this lack of privacy may come as a surprise, but what may be seen as a violation of security may, in fact, just be good business and unrealistic expectations by the user.[36]

II. Technologists & Lawyers, Tools & Technology

Just as the law provides a suite of tools to lawyers, from actions and affidavits to witnesses and writs, the technologist is provided with a toolkit containing solutions to the day-to-day problems of delivering information and content to global users. From local machines (physical or virtual) to off-premises IaaS, PaaS, SaaS, CaaS and Big Data solutions (See Table 2), technology has provided many new and different ways for people and devices to create, store, transport, and use data.

Term	**Definition**[37]
Infrastructure as a Service (IaaS)	Various providers offer a combination of physical and virtual computers (machines) onto which companies can install any necessary software packages. Rather than having physical machines located "on-premises," IaaS offers an easy way to lease collections of equipment on-demand to balance scalability and need requirements with cost and time, since costs are usually billed based on the amount of resources (even down to processor cycles) that are used.
Platform as a Service	Slightly more complete of a solution than IaaS, PaaS

'ordinary course of business' exception to the definition of device. . . . Second, Google contends that all Plaintiffs have consented to any interception.").

[36] *See id.* at *27 ("Google first contends that it did not engage in an interception because its reading of users' emails occurred in the ordinary course of its business.").

[37] Rackspace Support, *Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS*, Rackspace Support Network (Oct. 22, 2013), http://www.rackspace.com/knowledge_center/whitepaper/understanding-the-cloud-computing-stack-saas-paas-iaas.

(PaaS)	provides an install-base on the hardware that often includes databases, webservers, and operating systems. Windows Azure is a good example of a PaaS.
Software as a Service (SaaS)	A "hosted solution" where users are given access to a pre-defined application via the internet and usually pay on a per-user, per-month basis. Operation of the associated hardware and framework is the responsibility of the SaaS provider. Data is generally stored "in the cloud" in a shared environment next to other users/companies.
Compute as a Service (CaaS)	Distributed, shared compute environments have a recognized (to technologists) risk since data is comingled with other parties. Instead of uncontrolled IaaS, PaaS and SaaS solutions, some companies are offering solutions for different types of scalable cloud architecture that can be partially or wholly controlled by the purchaser. These deployment modes are differentiated as Private, Hybrid, Community and Public clouds.[38]

Table 2

Lawyers and analysts alike have become better familiarized with the vagaries of collection, preservation, review, and production of local data, but just in time to fall behind Moore's Law as technologists have introduced a more distributed environment. Need more computers? Why not pay Amazon® a few dollars for an IaaS scalable, remote, on-demand network? Need a software solution but don't want to host it yourself—a SaaS company is sure to oblige. Have streams of confusing data and aren't sure how to analyze it?—put it all in a Hadoop cluster[39] with a really hot pot of tea and watch what happens. Even better, when you are done with the project—or run out of money—just close your account, stop paying your bill, and everything disappears back into the nebulous world from whence it came.

[38] *What Is Cloud?*, IBM, http://www.ibm.com/cloud-computing/in/en/what-is-cloud-computing.html (last visited May 12, 2014); Brandon Butler, *AT&T Aims to Ease Private-To-Hybrid Cloud Transition*, NETWORK WORLD (Feb. 13, 2012, 5:48 PM), http://www.networkworld.com/article/2185810/cloud-computing/at-t-aims-to-ease-private-to-hybrid-cloud-transition.html.

[39] This refers to Apache Hadoop, which is "an open source software project that enables the distributed processing of large data sets across clusters of commodity servers." *What is Hadoop?*, IBM, http://www-01.ibm.com/software/data/infosphere/hadoop/ (last visited May 17, 2014). This gives businesses the ability to store and analyze all the data generated by their business to "put your big data to work for you." *Id.*

With these trends and capabilities, the law (and lawyers) must move to a more proactive stance. Ironically, law is not alone in being left behind; technology has also outpaced security initiatives. We have only to look to the recent data breaches experienced by Sony[40] and Target[41] to observe the ramifications and outcomes (legal, reputational, and financial). Contract law seems to offer some hope for the application of existing principles to both today's and tomorrow's technology, but the challenge for the legal profession is to apply these principles *before* the occurrence of a catastrophic event (financial or otherwise). Indeed, if it is the mission of Information System teams to make data available as broadly, cheaply, and streamlined as possible, then

- the legal team must measure the created risks against the possible positive and negative outcomes, and provide competent, judicious, and sage advice to potential adopters;
- the security team must adequately track usage and behaviors; and
- the forensic and eDiscovery teams must create repositories where data can be captured, held, and produced with ease, accuracy, and reliability.

All of this means that lawyers and the law must obtain *and maintain* technological competence sufficient to represent their client's best interests. Indeed, recent amendments to the American Bar Association's Model Rules of Professional Conduct now make competency in technology (in connection with client representation) an attorney's ethical obligation.[42] In an increasingly high-speed, interconnected world, there is no room to reflect on, or argue about, events from two years ago. Keeping in mind Moore's Law, with those two years of reflection, 730 days, 10^3 hours, 10^6 seconds and 10^{17} processor cycles have passed and computer speeds doubled—and with that power, many new technologies have been unleashed.

In all of this demand for proactive law, it still remains possible (at least for the moment) to apply old principles. Arguments of custody and control,

[40] Sony PlayStation users' data was exposed through an attacker's access to the backend database of the gaming servers, leading to the theft of personal information from 77 million user accounts. Liana B. Baker & Jim Finkle, *Sony PlayStation Suffers Massive Data Breach*, REUTERS (Apr. 26, 2011), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426.

[41] Target was the victim of a massive attack skimming credit cards from their Point of Sale system. Alastair Jamieson & Erin McClam, *Millions of Target Customers' Credit, Debit Card Accounts May Be Hit By Data Breach*, NBC NEWS (Dec. 19, 2013, 12:07 PM), http://www.nbcnews.com/business/consumer/millions-target-customers-credit-debit-card-accounts-may-be-hit-f2D11775203.

[42] Debra Cassens Weiss, *Lawyers Have Duty to Stay Current on Technology's Risks and Benefits, New Model Ethics Comment Says*, ABA JOURNAL (Aug. 6, 2012, 2:46 PM), http://www.abajournal.com/news/article/lawyers_have_duty_to_stay_current_on_technologys_risks_and_benefits/.

rights, protections, admissibility, and accessibility still apply—whether for a criminal prosecutor laying out a murder case with a CSI agent or a civil trial team preparing for a theft of trade secrets case. However, applying the law retroactively grows increasingly complex. As an example, consider Facebook's photo-tagging and facial recognition capabilities crossed with the proposed EU Privacy Laws[43]:

Situation: A U.S. citizen, on U.S. soil, in a public space, takes a photograph of an E.U. citizen and posts said photo to the Facebook page of a U.S. Facebook user. This picture is then used by Facebook to tag *other* photos of that person across the Internet.

Quandary: Does the E.U. right to be forgotten and data ownership laws (put simply) suggest that the E.U. citizen can demand that Facebook infringe on the rights of the U.S. citizen to remove a "legally" taken and posted photo? What about the other photos that Facebook was then able to tag based on the information posted by the U.S. citizen?

If the law does not carefully consider current and future technology but instead concentrates on the narrow and limited technologies of the past, more and more of these conflicts will arise. Because we have progressed from an age where transiting from New York to San Francisco in eighty-nine days[44] was a feat worthy of world-wide acclaim to an age where a packet of information can move between North America and India in around 270 ms (.0000031 days),[45] the law should move away from dealing with information access and instead consider information usage. It should also move away from dealing only with information instantiation to information movement and dissemination. Courts only decide cases brought before them—which means lawyers who try cases are contributing to the evolution of law in a retrospective manner, and are therefore contributing

[43] These proposed EU privacy laws would require organizations to remove personal data from their systems if the individual no longer wants their personal data to be processed and there is no legitimate reason for the organization to keep it (for which the burden of proof is on the organization to show that they need to keep the data). EUROPEAN COMM'N, HOW WILL THE DATA PROTECTION REFORM AFFECT SOCIAL NETWORKS? 1, *available at* http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf.

[44] This is in reference to the *Flying Cloud*, which set a world record by sailing from New York City to San Francisco in 89 days in 1851. *Clipper Ship*, ENCYCLOPEDIA BRITTANICA, http://www.britannica.com/EBchecked/topic/121871/clipper-ship#ref109219 (last visited May 17, 2014).

[45] *IP Latency Statistics*, VERIZON, http://www.verizonenterprise.com/about/network/latency/ (last visited June 5, 2014).

to the lagging response to new technology. Only by proactive, intelligent analysis of capabilities and possibilities, and either corporate self-governance or rapid adoption of regulatory requirements, can we hope to stop the divergent path of law and technology.

III. THE CONVERGENCE LANDSCAPE

Law, security, forensics, and eDiscovery must realize that they serve at least parallel, if not identical, and converging requirements and desired effects. Each exists for the protection of the innocent, assignment of responsibility, and discovery of the truth. If these fields work separately, advances in technology will easily surpass the independent ability of any one field, or perhaps any two. Forensics and discovery without security may leave nothing to discover. Security and discovery are needless without Law.

A. *Origin of Data*

In Part II, I qualified the assertion that it is possible to apply old principles with *for the moment*. Over the next few years, that "moment" will pass; inside of the next couple iterations of Moore's Law, there will be sufficient processor power, storage, and communication capability to make intelligent machines a thing of the present instead of the future. When this occurs, decisions are made not based on the limitations of some human-defined program, but by the decision matrix determined by, and written by, a computing device. We are already seeing computing devices that execute decisions where the logic for those decisions is impeccable (meaning that the decisions are based on correct mathematical models), but where the flexibility offered by the designer can be taken to include multiple options. When confronted with a potential collision, does a self-driving car make the decision to turn or stop in order to avoid a crash? Is the "lesser of two evils" hitting a pedestrian (less damage to the vehicle and passenger) or hitting a brick wall (more risk to passengers, but less risk to the pedestrian)? Does an IaaS hive in a data center that is losing power exercise its self-healing capabilities to move dependent virtual machines to alternate centers in London or Tokyo? Do (or should) data privacy considerations enter into the equation, or merely routing times, network traffic delays and the cost of power? Do natural gas futures on the NYSE end up controlling the decision matrix for where devices "decide" to do their processing based on some general criteria established by some long-lost program?

If we answer the questions above with the realization that society, at some point, can no longer unravel the web of programming to "blame" a decision on a person, or even a company, where do we attribute responsibility when data moves from country to country to find the best processing environments and perhaps is compromised along the way, or for casualties that might occur?

One cannot discuss the drivers for technological advances without considering computer games. Computer-controlled, or at least highly computer-reliant interactive methodologies of touching our pleasure-pain sensors have been the study of decades of research based on concepts grounded in the millennia.[46] Electrodes in mice, apes, and humans induce pleasure and pain, and easily make the jump into computer controlled reality (or virtual reality).[47] But when reality can be what a self-aware computer can make someone believe, or when someone's reality is controlled by titillation of their pleasure-pain centers, the law may have a problem finding examples in the physical world. "Gamers" that live, work, marry, and die entirely inside of a virtual world[48] may likewise face challenges when trying to apply physical-world laws, controls, and limitations on data custody, access, and even existence to their virtual world(s). All of this becomes another challenge for lawyers and represents a necessary convergence between the forensic collection and analysis of data; the electronic discovery, review, and production of data (real or virtual); the security around the creation, movement, and usage of data; and the law around the rights and privileges to and of the same.

The ultimate question may have already become, "where did the data come from?" In previous years, the "author" could eventually be tracked down. Whether it was chips in a stone tablet to ink on paper, sufficient research could ultimately determine the origin of the data in question and, with some similar degrees of reliability, the authenticity. With the shift to

[46] Adam Keiper, *The Age of Neuroelectronics*, THE NEW ATLANTIS, Winter 2006, at 4, 13, 15. One such philosophy that explored pleasure and pain is hedonism. *Hedonism*, INTERNET ENCYCLOPEDIA PHIL., http://www.iep.utm.edu/hedonism/ (last visited May 13, 2014).

[47] *See* Keiper, *supra* note 46, at 7–21 (discussing history of experimentation on pleasure and pain centers of the brain with electrodes). *See also* Tim Ferguson, *Virtual Reality Study Probes Brain Activity*, ZD NET (Feb. 24, 2011), http://www.zdnet.com/virtual-reality-study-probes-brain-activity-3040091925/ (discussing Swiss study exploring self-awareness through the use of virtual reality). *See also* Paul Marks, *Electrode Recreates All Four Tastes on Your Tongue*, NEWSCIENTIST (Nov. 20, 2013), http://www.newscientist.com/article/mg22029444.500-electrode-recreates-all-four-tastes-on-your-tongue.html#.U3hHSqDD_IU (discussing electrical stimulation through electrodes that recreate tastes in subjects).

[48] In the virtual online world *Second Life*, users create avatars that can carry out all the functions of real life. *Second Life*, WIKIPEDIA, http://en.wikipedia.org/wiki/Second_Life (last visited May 13, 2014).

electronic data, without the surrounding metadata, it may be not just difficult, but impossible, to establish origin or authenticity.

The "Hearsay" exclusionary rule provides generally that a statement will be considered hearsay if it is: (1) An assertive statement; (2) made by an out-of-court declarant; and (3) is being offered to prove the truth of the matter asserted therein.[49]

This concept, when considered in combination with the earlier discussions on the origins of electronic evidence, raises significant admissibility concerns that will need to be addressed by the courts.[50] In an electronic world, applying principles of law without addressing security and forensics (the provenance tracking origin and usage) can result in a morass of ESI that is deemed inadmissible hearsay because it lacks any sort of authenticity, chain of evidence, or reality. Failure to address these issues will lessen the likelihood of determining just who the declarant is in a hearsay evidentiary proffer. In the case of the Facebook "quandary," while clearly someone took and uploaded the picture, the subsequent data tagging and potential cross-border data explosion was done by machines choosing what faces looked most similar to the given face. This differs from the previous argument of machine-generated data[51] because of the very fuzzy logic introduced into the decision matrix to find *near* matches instead of *exact* matches. The arguments in *United States v. Washington*[52] are foundationally based on a machine making the same choice every time at the clear direction of a set of instructions. Movie claims of "self-awareness," such as those in *The Terminator* and *The Matrix* aside,[53] in the previous progression of Moore's Law, if not earlier, there are strong arguments that a combination of

[49] FED. R. EVID. 801.

[50] For a discussion of such concerns, see Steven W. Teppler, *Testable Reliability: A Modernized Approach to ESI Admissibility*, 12 AVE MARIA L. REV. 213 (2014).

[51] The argument was that machine-generated data was not hearsay because it was not a statement, as it came from a machine. *Machine-Generated Data Was Not a Statement and Raised No Hearsay or Confrontation Clause Issues*, FED. EVID. REV. (Dec. 12, 2008), http://federalevidence.com/blog/2008/december/machine-generated-data-was-not-statement-and-raised-no-hearsay-or-confrontation-c. Some authors have criticized this logic, noting that all data from machines originate from people at some point, whether the user inputting data or the programmer writing the code. *See* Teppler, *supra* note 50.

[52] In that case, the Fourth Circuit rejected the defendant's argument that toxicology results produced by lab equipment were hearsay statements offered by the lab technicians who operated the machines, because the lab technicians merely reported the results the machines gave. United States v. Washington, 498 F.3d 225, 227 (4th Cir. 2007).

[53] In both of these movies, machines gained a level of sentience, allowing them to think like humans. *Synopsis for* The Terminator, IMDB, http://www.imdb.com/title/tt0088247/synopsis?ref_=tt_stry_pl (last visited May 13, 2014); *Synopsis for* The Matrix, IMDB, http://www.imdb.com/title/tt0133093/synopsis?ref_=tt_stry_pl (last visited May 13, 2014).

well-designed programs, fast processors, and large storage have combined to give machines at least some freedom of choice, where "they" may not make the same decision every time or at least may not have the same data available to them within very short spans of time and therefore make different decisions based on the flood of data under review.[54] This variation may, in fact, be built into the code to allow for distributed answers preventing, for example, traffic congestion related to everyone getting the same route for rush-hour travel.[55]

Since technology in a vacuum has no association with forensics or law (and minimal use for security), security, forensics, and law must converge in order to provide a framework to answer future questions of law and to prevent gross abuses related to untraceable data and indeterminate losses. The best manner of this convergence will be through a combination of cross-discipline education and proactive planning.

B. *Creation, Collection, & Correlation*

The *creation* of data has also shifted, at a recent but indeterminate point in the past, from data produced by singularities (*e.g.* a person) to data produced by a more nebulous collection of entities (such as devices or crowds) with often little or no distinct individuals.[56]

Data is often purposefully anonymized in order to eliminate the distinction and provide a more general overview.[57] While it has proven possible to de-anonymize data again, the creator, or instantiator, of the data is often lost forever.[58] Big data, or the parallel clustering of multiple indexed storage repositories, provides the ability to store and search massive amounts

[54] Jean-Charles Pomerol, *Artificial Intelligence and Human Decision Making*, 99 EUROPEAN J. OPERATIONAL RES. 3, 4 (1997) (arguing that artificial intelligence should mimic individual humans' decision making, rather than following general processes, opening up the possibility for different decisions being reached).

[55] J.T. Barett, *How Does Google Detect Traffic Congestion?*, AZ CENTRAL, http://yourbusiness.azcentral.com/google-detect-traffic-congestion-17094.html (last visited May 13, 2014).

[56] SINTEF, *Big Data, For Better or Worse: 90% of World's Data Generated over Last Two Years*, SCIENCEDAILY (May 22, 2013), http://www.sciencedaily.com/releases/2013/05/130522085217.htm.

[57] Barett, *supra* note 55. However, there are limits to the ability to anonymize data. *See* Nate Anderson, *"Anonymized" Data Really Isn't—and Here's Why Not*, ARS TECHNICA (Sept. 8, 2009, 7:25 AM), http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/.

[58] The original collector of the data may be out of business, shielded by multiple layers or be a conglomeration of many different produces, and therefore lost from objective determination of the singularity.

of data from multiple sources.[59] Law, forensics, and security are all currently based on controlling and determining access to the data—and this stands in direct opposition to technology's presumed intent to provide open access to more data from more locations and by more things.

The ideas of creation, access, and collection of data are epitomized in the concepts of the IoT and crowd-sourced solutions. Gartner (a respected technology research firm) suggests that there will be twenty-six billion devices connected together into a web that we call the Internet by 2020.[60] This excludes personal devices, such as laptops or smart phones, and instead refers to devices that have their own reasons for connectivity.[61] Twenty-six billion devices are creating, collecting, and reading data streams and determining cooling patterns for homes, grocery purchases, highway speeds, and traffic flow or navigation routes.[62] Likewise, crowd-sourced solutions of everything from gene-splicing solutions[63] to speed-trap detection[64] results in a degree of anonymity and distribution to each input, and yet, the solution taken as a whole becomes a random group of unique answers converging on a desired effect. When life-critical or similarly vital actions are taken based on this input, it will eventually become the responsibility of law to decipher and untangle the web of input and decision matrices. From earlier premises and realizations, it should be clear that the law, at this point, will need the proactive input of security and forensics in order to have any degree of likelihood to collect appropriate data on which to act.

Combining advances in storage, data processing, and indexing (the ability to rapidly find stored data—think Google returning millions of search results in less than a second shown in Figure 2)[65] give the realistic possibility of correlating near-infinite sources together and developing decisions on that information. From these correlations, it would be theoretically possible to predict everything from performance to behavior and start asking questions

[59] *Big Data: What It Is and Why It Matters*, SAS, http://www.sas.com/en_us/insights/big-data/what-is-big-data.html (last visited May 13, 2014).

[60] *Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units by 2020*, GARTNER (Dec. 12, 2013), http://www.gartner.com/newsroom/id/2636073.

[61] *Id.*

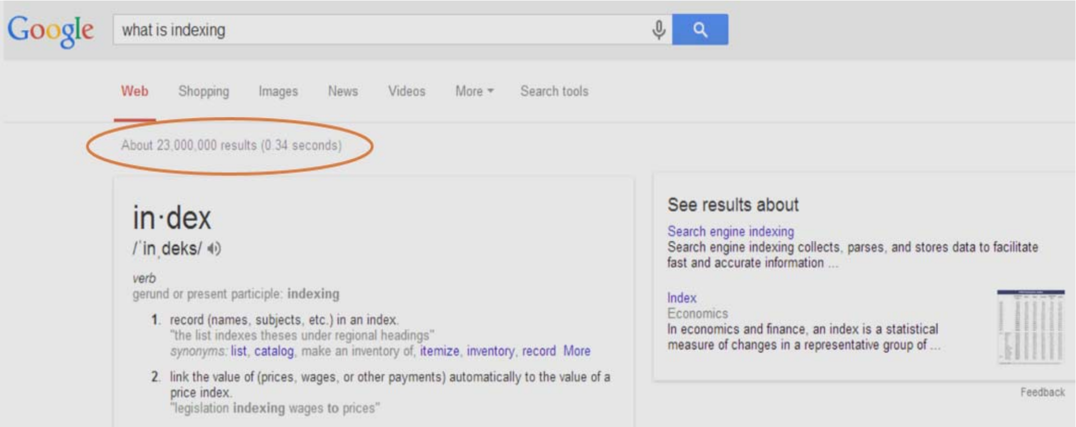
[62] *50 Sensor Applications for a Smarter World*, LIBELIUM, http://www.libelium.com/top_50_iot_sensor_applications_ranking/ (last visited May 15, 2014).

[63] Samuel Gibbs, *Phylo: Crowdsourcing Genetic Analysis Through Gaming*, SWITCHED (Dec. 1, 2010, 3:00 PM), http://downloadsquad.switched.com/2010/12/01/phylo-crowd-sourcing-genetic-analysis-through-gaming/.

[64] Chris Woodyard, *Radar Detectors Will Be Able to Warn Others of Speed Traps*, USATODAY.COM (Oct. 24, 2011, 9:06 AM), http://usatoday30.usatoday.com/money/autos/story/2011-10-24/radar-detector-crowd-sourcing/50888878/1.

[65] *See infra* Figure 2.

like the movie *Minority Report*.[66] There, precognitive law became a prevention tool instead of a reactive tool, with the mission to imprison people *before* they commit a crime.[67] Here, clearly, the idea of preemptive legal action moves too far, but the discussion no longer is directed to ensuring that metadata/tracking information exists, but actually taking action based on expected future behavior. If *that* is a bad idea, why would other behavior-predictive ideas be any better? Companies are examining concepts like predictive shipping and other Big Data mining opportunities as ways to make or save money.[68] Since financial considerations tend to be the primary driver for most corporate decisions in a capitalistic society, it becomes necessary for there to be a counter to the financial consideration and to keep the consumer/client/customer needs and safety in perspective.



About 23,000,000 results (0.34 seconds)

in·dex
/ˈinˌdeks/

verb
gerund or present participle: **indexing**

1. record (names, subjects, etc.) in an index.
"the list indexes theses under regional headings"
synonyms: list, catalog, make an inventory of, itemize, inventory, record More
2. link the value of (prices, wages, or other payments) automatically to the value of a price index.
"legislation **indexing** wages to prices"

See results about

Search engine indexing
Search engine indexing collects, parses, and stores data to facilitate fast and accurate information ...

Index
Economics
In economics and finance, an index is a statistical measure of changes in a representative group of ...

Figure 2

As the IoT generates data *on its own*, there is some degree of disassociation from the supposed owner of that information, as well as many questions of law about the associated usage, privacy, custody, and control of that information. We have:

[66] *Synopsis for* Minority Report, IMDB, http://www.imdb.com/title/tt0181689/ (last visited May 13, 2014).

[67] *Id.*

[68] One example of a company doing this is Amazon, who has filed a patent for a shipping system that would cut delivery times by predicting what buyers will buy before they buy it and shipping those items in their general direction before a purchase is even made. Natasha Lomas, *Amazon Patents "Anticipatory" Shipping—To Start Sending Stuff Before You've Bought It*, TC (Jan. 18, 2014), http://techcrunch.com/2014/01/18/amazon-pre-ships/.

- A convergence of interests between forensics, security, and law (with eDiscovery naturally protected by the relationship between the other three areas), and
- an area where law is the strongest (or only) force that can drive security and forensic proactive solutions.

Technologies included in Twitter and AOL® took years to cross the million user mark,[69] giving the trifecta of security, forensics, and law time to catch up with the offerings. Today, Instagram and applications such as Draw Something are forging past the million-user mark within months or even days![70] With this number of worldwide subscribers, retroactive application of solutions is no longer a simple process. Changes in anything from privacy policies to usage and access logs can cause major repercussions in functionality and brand. Where a team of less than 50 people, and sometimes less than five people, can affect the lives of millions,[71] trying to leverage yesterday's solutions of subpoenas and data requests against a "company" doesn't have the same impact as making those actions against a more stable and established corporate entity. Sometimes, since the new solution has leveraged other third-party solutions with their own set of privacy, access, and usage restrictions and capabilities, it may not be possible to comply with the requests.

CONCLUSION

Decisions addressing convergence and technology advancement issues and how to resolve them need to be made *now*. When bad technology practices affected tens, or even thousands of people, there arguably was time for recoverability from such bad decisions. As the speed of technological adoption increases along with the speed of technology development, undoing bad decisions becomes non-trivial and significantly impacts our lives. Decisions over privacy cannot be undone. Once something is moved onto

[69] AOL took nine years, Alex Cocotas & Henry Blodget, *The Future of Mobile [Slide Deck]*, BUSINESS INSIDER (Mar. 22, 2012, 8:44 PM), http://www.businessinsider.com/the-future-of-mobile-deck-2012-3?op=1, and Twitter took two years. Alyson Shontell, *Here's How Long It Took 15 Hot Startups to Get 1,000,000 Users*, BUSINESS INSIDER (Jan. 9, 2012, 8:01 AM).

[70] Instagram reached one million users after 2.5 months, Shontell, *supra* note 69, while Draw Something reached one million users in only nine days. Cocotas & Blodget, *supra* note 69.

[71] For example, one man, Ladar Levison, protected the users of his private email system from government intrusion by refusing to hand over to the government the security key for the system, despite a court order. Michael Phillips & Matt Buchanan, *How Lavabit Melted Down*, NEW YORKER (Oct. 7, 2013), http://www.newyorker.com/online/blogs/elements/2013/10/how-lavabit-edward-snowden-email-service-melted-down.html.

the World Wide Web (WWW), it becomes as much a part of our fabric as a television broadcast and a printed newspaper. It should be crystal clear that the opportunity for retraction has passed and that information sent out into the digital wilderness is "out there" forever with the added benefit of being indexed and cataloged for easy retrieval.[72] Without well-designed security, there will be no way to effectively *and reliably* provide computer forensics. The crime scene becomes a sterile room that offers no evidence: no footprints, no DNA, no video footage. Without forensics, the law has nothing from which to work except, perhaps, endless streams of conflicting testimony and contradictory or missing evidence. Lawyers, judges, courts, and boardrooms must work together to create a sustainable foundation from which technological advances can grow and flourish, while providing the framework for dispute resolution and litigant protection.

[72] *How Google Search Works*, GOOGLE, https://support.google.com/webmasters/answer/70897?hl=en (last visited May 15, 2014). However, it is not impossible to remove yourself from the internet. *See* Kim Komando, *How to Delete Yourself from the Internet*, USA TODAY (Jan. 25, 2013, 7:45 AM), http://www.usatoday.com/story/tech/columnist/komando/2013/01/25/komando-delete-yourself-internet/1852143/ (describing how to "disappear from the Internet").