Bloomberg BNA

Electronic Commerce & Law Report™

INTERNET OF THINGS

The Internet of Things has been called by the Industrial Internet Coalition a third revolution on par with the Industrial Revolution and Internet Revolution itself. The authors raise the issue of what such an additional explosion of data will do to the electronic discovery process, arguing that e-discovery law is better poised for this avalanche than it was for earlier onslaughts of new data, and that the Federal Rules of Civil Procedure may exclude much of that new data from discovery altogether.

Treading Beyond the Iota of Fear: eDiscovery of the Internet of Things

BY ELIZABETH MCGINN AND TY YANKOV

First came the Industrial Revolution. Then the Internet Revolution. And today we have made a firm step into the dawn of a third revolution called the ''Internet of Things'' or ''IoT.'' Or at least this is how IoT's arrival was put by the head of the Industrial Internet Consortium – founded in March 2014 by household-name companies like AT&T, Cisco, GE, Intel, and IBM to advance and coordinate the rapid rise of IoT.[1]

This is no hyperbole. In mid-2013, the Economist surveyed 779 executives from around the world about the extent to which their companies make use of IoT in their external products and services or internal operations and processes.[2] Almost all senior executives (96%) expected their business to be using the IoT in some respect within the next three years.[3] Indeed, Cisco forecasts that IoT will have an economic impact of over $14 trillion by 2022,[4] while per GE's prognosis IoT could add $15 trillion to the world economy over the next 20 years.[5]

In layman's terms, IoT represents the exciting and, for some, terrifying[6] ecosystem of interconnected sensory devices performing coordinated, pre-programmed—or even learned—tasks without the need for continuous human input.

Think Nest thermostats, which ''know'' when to expect you to come home. Now imagine your Fitbit activity tracker telling your Nest that it needs to turn the A/C down a bit lower than usual before you come home because you have had an exhausting run. Maybe your auto insurance premiums will be determined in part by your driving habits as transmitted by embedded sensors

Elizabeth McGinn is a partner and Ty Yankov is an associate in the Washington, DC and New York offices of BuckleySandler LLP. They advise clients on consumer financial services, e-discovery, and privacy-related issues. They may be reached at emcginn@buckleysandler.com and tyankov@buckleysandler.com, respectively.

[1] Richard Mark Soley, Industrial Internet Consortium, *The Industrial Internet: A Sense of the Future* (Sept. 15, 2014), http://www.industrialinternetconsortium.org/tx-14/presentations/Soley_Opening_Keynote-9-15-14.pdf.

[2] Clint Witchalls, *The Internet of Things Business Index: A Quiet Revolution Gathers Pace*, The Economist (Oct. 29, 2013), http://www.economistinsights.com/analysis/internet-things-business-index.

[3] Id.

[4] Joseph Bradley et al., *Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion: More Relevant, Valuable Connections Will Improve Innovation, Productivity, Efficiency & Customer Experience 1-18* (Cisco, White Paper, 2013), http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf.

[5] Peter C. Evans and Marco Annunziata, *Industrial Internet: Pushing the Boundaries of Minds and Machines 3-34* (Nov. 26, 2012), http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf.

[6] *Invasion of the Data Snatchers*, American Civil Liberties Union, https://www.aclu.org/technology-and-liberty/invasion-data-snatchers.

 ISSN 1098-5190

in your vehicle,[7] and your homeowner's insurance premium might be lowered if you could show there is usually someone home.

As one technology journalist summed it aptly, ''these connected objects will act more like a swarm of drones, a distributed legion of bots, far-flung and sometimes even hidden from view but nevertheless coordinated as if they were a single giant machine.''

So perhaps it is no exaggeration that IoT will soon impact nearly every facet of industrialized societies. In many ways it already has. But for litigators conducting e-discovery in the IoT world, this is where the fascination seems to end and the headaches begin.

Indeed, a review of opinions on IoT's anticipated impact on e-discovery appear to thumb the scale in favor of trepidation. As one e-discovery expert remarked recently, ''[e]ventually there will be as much data as 'molecules in the universe,' '' much of which ''might be of interest to various kinds of lawsuits.''[9] And another commentator put it memorably: ''[T]he deluge of data discoverable in legal actions will dwarf the data tsunami that is seemingly engulfing litigation teams today . . . . The number of 'rocks' that e-discovery professionals will be called upon to collect, analyze and produce data from will be infinite . . . . It will be a brave, new world of digital law and practice.''[10] In turn, skeptics are admonished for not thinking big and are reminded of how previous ''insular thinking'' underestimated the impact that other recent technological advents – such as social media discovery – have had in litigation.[11]

Let's take e-eath. IoT's impact on e-discovery will likely be disproportionately muted compared to its impact on the economy and society as a whole. Even assuming that IoT data will swim in relevance, the e-discovery community, and our discovery system as a whole, is better prepared to respond to this round of anticipated avalanche than it was during the Internet Revolution, when not long ago many lawyers were printing and Bates stamping e-mailed attachments from their inbox.

Without a doubt, the litigant's primary challenge of IoT discovery is preservation and collection of IoT data. To be sure, commentators have noted that IoT devices are not designed with data preservation or collection in mind.[12] But neither were backup tapes. Nor Facebook or Twitter. Although innovation in e-discovery necessarily lags behind the innovation of the underlying technology, it has always solved the problem that it had created. There's no reason to believe the IoT experience will be materially different. But until that day arrives, courts should avail litigants of protections against disproportionate e-discovery efforts.

IoT data is radically different from current forms of common electronically stored information (''ESI''): it is not created by humans. It does not reflect Joe's direct communication with Jane. Rather, it represents device X gathering data about Joe, ultimately communicating with a centralized database and/or another device about Joe. As a result, from a discovery perspective, much of the generated data by an IoT device may no longer reside within the device after it is transmitted. In most cases, the data will be stored in the cloud, where the order of resulting automated activities will be directed by the artificial intelligence of the cloud.[13] So, preservation efforts would go beyond placing a litigation hold or flipping the ''off switch''[14] of the device itself. These attributes raise a number of preservation conundrums.

The responding litigant may not have the requisite control over IoT data to preserve it.

The first difficulty to preservation concerns the primary question of control of the cloud data, which is not unique to IoT.[15] Businesses are investing billions into IoT not only because of their profit expectations from the one-time sale of an IoT device, but also from having unfettered access to the valuable data produced by the devices.[16] Google did not purchase Nest for $3.2 billion only because it is cool to control thermostats from a phone. Google already knows a lot about its users from scanning Gmail accounts to present users with pertinent ads, and now it will know when individuals are statistically likely to leave their house.

Similarly, the technology giant probably did not buy Boston Dynamics because its robotic cheetahs are fun. While the company has been mum about its intentions, by connecting multiple communicating devices into a single automated ecosystem, one can create not only a very accurate data map about a person's past and present activity, but also dispense a sensory device—robotic or otherwise—to cater to the person's *anticipatory* needs. But will you have control over your personal data map?

Consider that wireless pacemakers, which allow third parties to wirelessly monitor one's heart, may soon become the norm.[17] Will the person, the healthcare provider, or the device manufacturer control this data?

---

[7] National Association of Insurance Commissioners, *Usage-Based Insurance and Telematics*, The Center for Insurance Policy and Research, http://www.naic.org/cipr_topics/topic_usage_based_insurance.htm (last updated Oct. 29, 2014).

Bill Wasik, *In the Programmable World, All Our Objects Will Act as One*, Wired (May 14, 2013), http://www.wired.com/2013/05/internet-of-things-2/.

[9] Mark Gerlach, *The Internet of Things and EDiscovery*, Law Technology News (Nov. 21, 2014), http://www.lawtechnologynews.com/id=1202677077877/The-Internet-of-Things-and-EDiscovery-?slreturn=20150102182730#ixzz3QAuB3DrR.

[10] Michelle Lange, *How the ''Internet of Things'' Will Impact eDiscovery*, JDSupra Business Advisor (Mar. 6, 2014), http://www.jdsupra.com/legalnews/how-the-internet-of-things-will-impact-12960/.

[11] *Id.*

[12] Mark Gerlach, *The Internet of Things and E-Discovery*, Law Technology News (Nov. 21, 2014), http://www.lawtechnologynews.com/id=1202677077877/The-Internet-of-Things-and-EDiscovery-.

[13] Bill Wasik, *In the Programmable World, All Our Objects Will Act as One*, Wired (May 14, 2013), http://www.wired.com/2013/05/internet-of-things-2/.

[14] *See, e.g.*, *Mosaid Tech., Inc. v. Samsung Elecs. Co., Ltd.*, 348 F. Supp. 2d 332, 339 (D. N.J. 2004).

[15] *See, e.g.*, *Brown v. Tellermate Holdings Ltd.*, No. 2:11-CV-1122, 2014 WL 2987051, at *10 (S.D. Ohio July 1, 2014) (imposing sanctions for litigants' failure to preserve cloud data when the party had control over the data as evidenced by its contract with the cloud provider.).

[16] Harvard Business Review Staff, *With Big Data Comes Big Responsibility*, Harvard Business Review (Nov. 2014 Issue), https://hbr.org/2014/11/with-big-data-comes-big-responsibility/ar/1.

[17] Ben Gruber, *First Wi-Fi Pacemaker in US Gives Patient Freedom*, Reuters (Aug. 10, 2009), http://www.reuters.com/article/2009/08/10/us-pacemaker-idUSTRE5790AK20090810.

  ECLR ISSN 1098-5190

While the implications of IoT may guarantee full employment to privacy and data security lawyers, to name a few, for the litigator this may be but a straightforward threshold question, hopefully with a straightforward answer based on the contractual agreements in place.[18]

It may be difficult to target only the potentially relevant IoT data for preservation.

Yet unlike most clouds, the IoT cloud serves not only as a mere storage facility of the transmitted data, but also as a computing medium that manipulates the data transmitted by the devices.[19] This distinction may go to the heart of relevance: the data transmitted by the device to the cloud about Joe's activity may be relevant, but the way it's manipulated by the cloud intelligence to direct the automated response might not be relevant to the extent it goes beyond manually inputted user settings. And vice versa: if only the computing algorithm of the cloud is at issue, then the underlying IoT data it's fed may be irrelevant. Can the two be preserved, collected, and analyzed independently?

One final set of questions go to the heart of spoliation claims: does the cloud intelligence manipulate the data it receives in a way that irreversibly alters it as part of its routine operation? How long are historical transmissions retained? And would ''flipping the off switch'' at the cloud level to prevent such alteration pose an undue burden by potentially stalling enterprise-wide activities?

Preservation of IoT may be limited by the proposed revisions to the Federal Rules of Civil Procedure.

Although these challenges are far from superficial, litigants may soon have powerful legal tools for handling IoT preservation. Perhaps the most potent limitation to a party's preservation and collection obligation of IoT data may rest in the timely proposed revisions to the Federal Rules of Civil Procedure, which are widely expected to take effect by the end of 2015. Mindful of litigants' inclination to over-preserve evidence,[20] the Rules Committee seeks to clarify and limit litigants' preservation obligations in three important ways.

First, revised Rule 26(b) will rein in past scope creep by clarifying that discoverability does not extend to issues beyond the parties' claims or defenses, eliminating litigants' ability to procure broader subject matter discovery for good cause.[21] This may contain the sea of potentially relevant IoT data to a more manageable pond – perhaps in some cases even closing the door to IoT discovery altogether.

Key Proposed Revisions to Federal Rules of Civil Procedure Affecting IoT Discovery

- Proposed Rule 26(b) limits discoverability to issues within the parties' claims or defenses, eliminating broad subject matter discovery
- Proposed Rule 26(b)(2)(i) redefines the scope of discovery to include a proportionality principle
- Proposed Rule 37(e) extends the proportionality principle to the duty to preserve evidence
- Proposed Rule 26(b)(2)(B) reaffirms the allocation of expenses as a potential protective order remedy

Second, proposed Rule 26(b)(2)(1) will place proportionality squarely within the definition of scope of discovery. Under the proposed rule, even if IoT data is relevant to a claim or defense, its discovery will have to be ''proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.''[22] Although the current Rule 26 also contains a similar provision,[23] the Rules Committee explicitly added the word ''proportional'' and moved the provision into the definition of scope of discovery in response to observations that the proportionality doctrine has not gained sufficient traction.[24]

Third—and most critically—the proposed revision to Rule 37(e) will extend proportionality to preservation, perhaps due to the Rules Committee's recognition that the initially envisioned safe harbor has dried up into a puddle.[25] This change is particularly noteworthy because some courts have been reticent to expand the proportionality principle to preservation.[26] The proposed revision to the Rule would restrict the imposition

---

[18] *See, e.g.*, *Brown v. Tellermate Holdings Ltd, supra* n. 16.

[19] *In the Programmable World, All Our Objects Will Act as One*, *supra* n. 14.

[20] Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, *Summary of the Report of the Judicial Conference Committee on Rules of Practice and Procedure*, (''*June 2014 Rules Report*''), Appendix B-14 (''Resolving the circuit split with a more uniform approach to lost ESI, and thereby reducing a primary incentive for over-preservation, has been recognized by the Committee as a worthwhile goal.''), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/ST09-2014.pdf.

[21] *June 2014 Rules Report*, at B-43 (noting that the language is rarely invoked and that ''[p]roportional discovery relevant to any party's claim or defense suffices, given a proper understanding of what is relevant to a claim or defense.'').

[22] Proposed Fed. R. Civ. P. 26(b)(2)(1).

[23] *See* Fed. R. Civ. P. 26(b)(2)(C)(iii).

[24] *June 2014 Rules Report*, at B-2 (noting that the participants of the 2010 Duke Conference reached a ''near-unanimous agreement . . . that the disposition of civil actions could be improved by advancing cooperation among parties, proportionality in the use of available procedures, and early judicial case management.'').

[25] *Summary of the June 2014 Rules Report*, p. 14 (''Since the rule's adoption, it has become apparent that a more detailed response to problems arising from the loss of electronically stored information (ESI) is required.'').

[26] *See Pippins v. KPMG LLP*, 279 F.R.D. 245, 255 (S.D.N.Y. 2012) (internal citations and quotation marks omitted) (''[P]roportionality may prove too amorphous to provide much comfort to a party deciding what files it may delete or backup tapes it may recycle before that party files a motion for a protective order seeking to have a court define its preservation obligations. Accordingly, until a more precise definition is cre-

of sanctions—or even curative measures—for lost ESI unless the party seeking relief can show that the responding party failed to take ''reasonable steps'' to preserve the ESI in the ''*anticipation* or conduct of litigation.''[27] Note that the proposed change would effectively limit the availability of post-litigation remedies to pre-litigation conduct.

While ''reasonable steps'' is not a defined term, it appears that the Rules Committee seeks to bypass a line of cases following the *Pension Committee*[28] view that ''[o]nce the duty to preserve attaches, any destruction of documents is, at a minimum, negligent.''[29] Instead, the proposed Rule would build a new *de facto* safe harbor based on reasonableness of preservation, with proportionality offered as but one factor.[30] Moreover, even if the ESI loss stemmed from a party's failure to take reasonable preservation steps, the revised Rule would permit *curative* measures and only upon a finding of prejudice to the other party,[31] with sanctions reserved if one ''party acted with the intent to deprive another party of the information's use in the litigation.''[32]

With the fear of spoliation sanctions removed from its prominent perch, the responding party need no longer reflexively succumb to preserve more than is reasonable. From among all of ESI, few, if any, can match the costs and challenges of IoT preservation. So, as the ''avalanche'' of IoT data starts coming down the mountain, courts should not pressure the litigants into keeping it on the slopes.

IoT data may be reasonably inaccessible.

Finally, even if IoT must be preserved, it does not necessarily mean that it must be collected. Counsel may have strong arguments that IoT data is not reasonably accessible under Rule 26(b)(2)(B) and may be further subject to cost shifting under proposed Rule 26(c)(1)(B), which would explicitly authorize allocation of expenses in a protective order. Without a doubt, the case law will need to be updated to reflect the new challenges of IoT. Over a decade has passed since the *Zubalake* court noted that whether ESI is accessible or inaccessible ''turns largely on the media on which it is stored,''[33] a distinction that turns on whether the data needs to be manipulated or restored in any way in order to be usable. ''Backup tapes must be restored . . . fragmented data must be defragmented, and erased data must be reconstructed. That makes such data inaccessible.''[34] There's little reason to doubt that courts will extend this analysis to IoT data, even recognizing that, despite its unique properties, not all IoT is created equal.

In sum, IoT's impact to data preservation and collection in e-discovery will be more muted that many fear, in large part due to the anticipated adoption of the proposed revisions to the Federal Rules as applied to the unique challenges of its preservation and accessibility.

Reviewing IoT data may prove less costly than e-mail review.

But what about review costs of IoT data? Document review costs can be substantial, with one prominent study pegging them at an average of 73% of all e-discovery expenses.[35] But does this mean that, in a world inundated with ''smart'' common objects, litigants should brace for even higher review costs?

As IoT fully arrives, the leave-no-stone-unturned types will be in for a surprise as they discover that the stones become fully covered by grains of sand. But if IoT lives up to its promise of breaching the ESI dam, responding parties will be well-positioned to raise the levees without expending unreasonable efforts to produce it.

We think not. In most cases, we anticipate that the costs of IoT discoverability will be heavily weighted towards expenses associated with preservation and collection rather than of review and production because IoT data (1) lacks intricate communicative complexities of human-generated documents, (2) is not conducive to linear and costly document-by-document review, and (3) is highly unlikely to contain privileged information. Indeed, for the reasons below we believe that IoT review costs in the long run will prove to be proportionately lower than the review costs associated with a comparable e-mail collection.

First, the reason document review costs are so high at present is that human-generated data requires human intelligence to determine relevance. This is true even when relying on predictive coding, whose efficacy rests on iterative human input to ''teach'' the software what is relevant. But these considerations should not apply to IoT data: it is generated by machines and thus best reconstructed by machines. By design, IoT data is highly standardized in order to work for its intended purpose: each sensory device must gather and transmit uniformly formatted data to the cloud in order for the cloud intelligence to direct a specific action efficiently. Put differently, the beauty of IoT lies in its orderly complexity. Lawyers should use that to their advantage.

As a result, the most efficient way to reconstruct the collected data might be to repurpose the cloud intelligence to assist the lawyers in understanding what the data means. Easier said than done, perhaps, but it may

ated by rule, prudence favors either retaining all relevant materials, or swiftly moving for a protective order.'').

[27] Proposed Fed. R. Civ. P. 37(e) (emphasis added).

[28] *Pension Comm. v. Banc of America Sec.*, 685 F. Supp. 2d 456, 465 (S.D.N.Y. 2010), *abrogated by Chin v. Port Auth. of N.Y. & N.J.*, 685 F.3d 135 (2d Cir. 2012).

[29] *Summary of the June 2014 Rules Report*, p. 15 (Noting parties' ''tendency to over preserve ESI out of a fear of serious sanctions if actions are viewed in hindsight as negligent.'')

[30] *See* June 2014 Rules Report at B-61-62.

[31] Proposed Fed. R. Civ. P. 37(e)(1).

[32] Proposed R. 37(e)(2).

[33] *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 318 (S.D.N.Y. 2003).

[34] *Id.* at 320.

[35] Nicholas M. Pace & Laura Zaleras, *Where the Money Goes; Understanding Litigant Expenditures for Producing Electronic Discovery*, xiv (2012).

  ECLR ISSN 1098-5190

be more efficient than the alternatives: building specific tools to handle each IoT collection set with its own separate formatting intricacies, or manually trying to make sense of the data. This prescription invites the obvious question of asymmetrical access to the underlying technology: whether and how to allow the receiving party also to understand the produced data. Thus, in some cases, it may be entirely appropriate for the responding party to simply offer the IoT data for the requesting party's inspection rather than to review and produce it. We expect that litigators will have the foresight to discuss such matters during the meet-and-confer conference.

Second, it is true that a higher data size for collected ESI usually corresponds to a higher number of documents to review. But this would not necessarily hold true for IoT data, which is better viewed as one data set consisting of database entries, rather than documents or pages to review. And in our experience, a larger database is not necessarily more difficult to analyze than a smaller database, all else being equal. In a way, IoT data paints a pattern of one's activity as logged by the sensory devices. A picture—one that can be worth a thousand bytes or a million bytes—is still a picture. The litigator may only need to zoom in with the help of software.

Consider for instance one Dutch startup, which made news in 2010 after implanting cattle's ears with sensors to allow farmers to monitor cows' health and track their movement. On average, each cow generated about 200 megabytes of information a year.[36] Unlike document-based ESI, we suspect that the combined information from 1,000 cows would likely not cost ten times more to analyze than that of 100 cows, for the additional data points would offer additional detail but not necessarily greater complexity as to where the cows have been.

Finally, there's the mother of all fears: disclosing privileged information and the potential for subject matter waivers. Or in the case of IoT, the virtual lack thereof. It may be true that with the increasing amounts of ESI, the inadvertent disclosure of privileged material is virtually inevitable.[37] To guard against privilege waivers, parties have been encouraged to enter into clawback agreements and seek Rule 502(d) protective orders at the outset of discovery, especially when utilizing technology assisted review tools such as predictive coding.[38] But as one commentator aptly noted, the primary reason litigants are unwilling to rely on these alone is because ''in most cases the damage caused by disclosure of some privileged communications cannot be fully repaired by clawback agreements and orders, even when they are enforced'' for one cannot un-ring the bell after disclosing a secret.[39] Such observations have led some commentators to recommend more stringent—read, costly—review protocols when utilizing predictive coding for privilege review.[40]

But thankfully, IoT data would be very unlikely to contain privileged information. After all, you won't be (or shouldn't be) asking your SmartSlippers™ to dispense legal advice. That said, it is not inconceivable that IoT devices would never be used for communicating privileged information. For example, the CEO of one technology company has set up his office to automatically text his wife when he leaves the office[41] and thus might seek to invoke spousal privilege if this communication were to become relevant to a subsequent lawsuit.[42] But on balance, unlike most other ESI, lawyers would generally know whether to expect privileged information in an IoT collection *before* having to review and analyze it *in toto*.

As the science fiction writer William Gibson once said: ''The future is already here. It's just not evenly distributed yet.''[43] The IoT has made its splash, driven by our insatiable desire for ''smart'' things in a quest for convenience and efficiency. What is born in the laboratories is spilling into our everyday lives, and from our everyday lives into, well, litigation. While the purported relevance of IoT data will be restrained only by the unbridled imagination of the requesting party, its discoverability should be limited to proportionality.

As IoT fully arrives, the leave-no-stone-unturned types will be in for a surprise as they discover that the stones become fully covered by grains of sand. But if IoT lives up to its promise of breaching the ESI dam, responding parties will be well-positioned to raise the levees without expending unreasonable efforts to produce it.

---

[36] *Augmented Business*, The Economist, Nov. 4, 2010.

[37] Dennis R. Kiker, *Waiving the Privilege in a Storm of Data: An Argument for Uniformity and Rationality in Dealing with the Inadvertent Production of Privileged Materials in the Age of Electronically Stored Information*, 12 Rich. J. L. & Tech. 15, 2 (2006).

[38] *See* Evan Koblentz, View from the Bench: Judges on E-Discovery at LegalTech Day Two, Law Technology News, (Jan. 31, 2013) available at Lexis doc-id (#1202586387206#) (Judge Peck opining that he would consider it malpractice if counsel did not consider seeking a Rule 502(d) order at the outset of discovery).

[39] Ralph C. Losey, *Predictive Coding and the Proportionality Doctrine, A Marriage Made in Big Data*, 26 Regent U. L. Rev. 7, 56 (2014).

[40] *See, e.g.*, Manfred Gabriel, Chris Paskach, David Sharpe, *The Challenge and Promise of Predictive Coding for Privilege*, Univ. of Md. Inst. For Advance Computer Studies (June 14, 2013), http://www.umiacs.umd.edu/~oard/desi5/research/Gabriel-final2.pdf (recommending significantly increasing sample sizes of predictive coding seed sets to achieve recall levels of 95-99% for privileged documents).

[41] Bill Wasik, *In the Programmable World, All Our Objects Will Act as One*, Wired (May 14, 2013), http://www.wired.com/2013/05/internet-of-things-2/.

[42] Whether this privilege claim will be successful and will satisfy the confidentiality prong is an important question that is beyond the scope of this article.

[43] Pagan Kennedy, *Reviewing Realities, William Gibson's Future Is Now*, The N.Y. Times, Jan. 15, 2012, at BRI.