Mark Holst-Knudsen likes to joke that Thomas Publishing Co. is the oldest internet company known to man, but in a sense, he's not far off. Founded in 1898, it published the Thomas Register of American Manufacturers, a multivolume directory of distributor, manufacturer, and service company information that helped connect buyers and sellers of industrial products.

So how did Thomas Publishing Co., known throughout the past century for its “big green books” on industrial product information, become the grandfather of internet businesses? It thrived by making the daunting leap from old-world physical media headfirst into the digital age, says Holst-Knudsen.

The Industry of Online Directories
Since 2006, when Thomas Publishing released its final edition of the Thomas Register of American Manufacturers, “we’ve been lock, stock, and barrel, 100% an internet company,” says Holst-Knudsen. And it’s been a successful reorientation. The company now has more than 700,000 different suppliers for its users to call upon, and the site receives 2 million user sessions a month. “[W]e’re one of the few companies that has made a complete and successful transition from traditional media in the print world to now, internet,” he says.

In 1898, the mission of the company was exactly the same as it continued on page 32.

Global Efforts to Redefine Privacy in the Age of Big Data
by NANCY K. HERTHER

In 2012, retail giant Target was outed in The New York Times for its development of algorithms that were able to identify a teen as pregnant before she was even able to tell her parents herself (nytimes.com/2012/02/19/magazine/shopping-habits.html). To retailers, it seems “new parents are [their] holy grail,” and being able to zero in on them early on allows a company to build incentives to hopefully lure those customers into patterns of regular continued on page 34.

Streaming Video in Public Libraries
by BRANDI SCARDILLI

In the beginning, libraries lent books. Fast-forward to present day, and patrons can borrow all kinds of things from the library, including books, ebooks, audiobooks, CDs, and DVDs. The newest available format for patrons is streaming video, which is quickly gaining traction in public libraries across the country. Several librarians shared their experiences with streaming video lending, so institutions thinking about implementing their own programs know what to expect.

Deciding on a Service
Boston Public Library (BPL) surveyed its patrons in early 2014 and found that access to streaming videos was one of the top-requested services, says Laura Irmscher, chief... continued on page 36.
people's phones and computers. Even local and state governments in the United States are snapping up surveillance technology ranging from drones to automated license plate readers that allow them to keep tabs on citizens' movements in ways never before possible.

The High Cost of Lost Privacy

"Admittedly," says Angwin, "it can be difficult to demonstrate personal harm from a data breach. ... But on a larger scale, the answer is simple: Troves of personal data can and will be abused." This Big Brother aspect of life today is something that author Mark Dice presents in his 2011 book Big Brother: The Orwellian Nightmare Come True. "Orwell's description of Big Brother," Dice writes, "was chillingly accurate, and perhaps not as horrific as the reality we may one day face. Like a Pandora's box once much of this technology is created, there will be little hope of stopping or even regulating it." However, today, there are important efforts underway to look at technology and privacy both here in the U.S. and in other parts of the world.

The Electronic Frontier Foundation (EFF) has established a ratings system to gauge how well major internet search engines and social media sites protect user privacy. The 2014 version of the report "Who Has Your Back: Protecting Your Data From Government Requests (eff.org/who-has-your-back-2014) gave the highest ratings to Apple, CREDO Mobile, Dropbox, Facebook, Google, Microsoft, SonicNet, Twitter, and Yahoo. Some strongly criticized several of the choices (bit.ly/1hogzdz); however, the foundation stands by its six-point criteria used to evaluate companies.

Laws that allow expungement (the sealing or erasure of some minor offense, treating the event as if it never occurred) or legal pardons have been intended to give people, with cause, a second chance in which their past is removed from public record. However, in our current environment, there is little chance of anyone being able to have his past forgotten—whether the information is true or untrue. As a CNN.com headline proclaimed last year, "Privacy? Forget It, We're All Celebrities Online Now" (cnn.com/2013/06/12/tech/social-media/internet-privacy-divide).

"You have zero privacy anyway," Scott McNealy, then-CEO of Sun Microsystems told a group of reporters in 1999. "Get over it" (archive.wired.com/politics/law/news/1999/01/17538). In response to this assertion, PC World's Stephen Manes wrote: "He's right on the facts, wrong on the attitude. It's undeniable that the existence of enormous databases on everything from our medical histories to whether we like beef jerky may make our lives an open book, thanks to the ability of computers to manipulate that information in every conceivable way. But I suspect even McNealy might have problems with somebody publishing his family's medical records on the Web, announcing his whereabouts to the world, or disseminating misinformation about his credit history. Instead of 'getting over it,' citizens need to demand clear rules on privacy, security, and confidentiality" (archive.today/JCLw1). Fifteen years later, we now face a future with wearable computers monitoring our every move and heartbeat, and drones are providing information on our every action—making the need for a workable solution all the more imperative.

From PATRIOT Act to FEDOM Act

Congressman Jim Sensenbrenner (R-Wis.) introduced the USA PATRIOT Act in the U.S. House of Representatives soon after 9/11 "as a method to help keep America safe by enhancing the tools our law enforcement officials could use to thwart another terrorist attack" (sensenbrenner.house.gov/biography). However, he came to believe that the inherent checks and balances in our system of government "only work when the other two branches do oversight on the others, and all three failed." Speaking at the University of Minnesota in April, Sensenbrenner also noted that this fact "is responsible for what has happened. NSA [National Security Agency] is out of control." Asked if we are presently in a constitutional crisis, he responded that "if the USA FEDOM Act passes, no, we can correct the problems and strike a balance" that protects both public safety and individual rights. However, "if the law doesn't pass, I believe this represents a serious crisis to our system of governance."

Edward Snowden, whose leaked documents have laid bare the extent of surveillance and lack of oversight, "had higher security status than Judith" (sen.sensenbrenner.house.gov/biography). However, he came to believe that the inherent checks and balances in our system of government "only work when the other two branches do oversight on the others, and all three failed." Speaking at the University of Minnesota in April, Sensenbrenner also noted that this fact "is responsible for what has happened. NSA [National Security Agency] is out of control." Asked if we are presently in a constitutional crisis, he responded that "if the USA FEDOM Act passes, no, we can correct the problems and strike a balance" that protects both public safety and individual rights. However, "if the law doesn't pass, I believe this represents a serious crisis to our system of governance."
In an article in The Guardian, author Dan Roberts says that key segments of the act, amending the PATRIOT Act, include the following:

- Place more onus on intelligence agencies to show they are looking for specific suspects and do not inadvertently sweep up information on innocent Americans.

- The attorney general would be required to publicly disclose decisions by the Foreign Intelligence Surveillance (Fisa) court that contain a significant construction or interpretation of law, but may continue to classify confidential parts.

- Internet and telephone companies that received Fisa court orders would be allowed to report the number of Fisa orders and national security letters complied with, and [the] number of users on whom information was demanded.

- Create an office of special advocate within the Fisa court who would have standing to appear to represent the public and privacy concerns.

- Prevent intelligence agencies from "reverse targeting" that may allow them to intercept email and internet communications of Americans.

- Title 4 of Fisa, known as the pen register and trap-and-trace provisions, would be amended to make sure the government does not just rebuild its metadata dragnet using different authorities.

- End "secret laws" being made behind closed doors by the Fisa courts and the intelligence community.

Many organizations, including the American Library Association (ALA), American Association of Law Libraries, American Civil Liberties Union, and Association of Research Libraries, pushed for even greater restrictions and transparency in a joint letter, noting that "while the bill makes significant progress in ending the bulk collection, we strongly believe that several technical corrections and clarifications to the bill are required if Congress is to help ensure that the bill language is not misinterpreted and its stated goal of ending bulk collections is met" (bit.ly/1meSTOk). Even though a somewhat watered-down version of the bill (beta.congress.gov/bill/113th-congress/house-bill/3361/text) passed in the House (with changes decried by many former supporters), it still needs to pass in the Senate and then go to a joint committee to work through differences in the legislation as passed before it can even get to the White House for a signature.

The European Union Acts to Protect Internet Privacy

In a world in which we can now not only be quoted but misquoted and also connect to others yet be constantly under surveillance, governments as well as individuals are working to deal with the ramifications and to understand and perhaps control the seemingly unstoppable pace of technology. The revelations that have come from the documents released by Snowden have resulted in a cascade of responses. Vladimir Putin says that the internet is, at its heart, some type of "CIA project" that requires control from other countries over their own territories (aje.me/1rooVNX). In an article in The Guardian, author Ewen MacAskill notes, "A purely Russian-run system could make it easier for the Russian intelligence services to monitor and control traffic" (theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia). And it's not just Russia that is concerned. "The idea of breaking up the internet has gained ground in Germany, Brazil and elsewhere round the world in the light of the revelations by whistle-blower Edward Snowden about the extent to which the US National Security Agency has infiltrated Facebook, Skype and other social media," writes MacAskill.

The United Nations' (UN) Universal Declaration of Human Rights, which was adopted by the world body in 1948, affirms in Article 12 that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (un.org/en/documents/udhr). Although the UN hasn't undertaken any work in the area of internet privacy, many countries now have.

On May 13, the Court of Justice of the European Union (EU) ruled that people now have the "right to be forgotten." The case involved Google's search engines continuing to display information on a Spanish man's past debts that no longer was true and affected his privacy and reputation. The court ruled that "if, following a search made on the basis of a person's name, the list of results displays a link to a web page which contains information on the person in question, that data subject may approach the operator directly and, where the operator does not grant his request, bring the matter before the competent authorities in order to obtain, under certain conditions, the removal of that link from the list of results" (curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf).

Although many U.S. companies and publications cried foul, Slate's Eric Posner believes that "much of the case turns on technical issues, such as whether a search engine is a 'processor' of personal data under the law (it is). The bottom line, however, is that Google must remove links to Web pages that contain personal information unless the public's interest in access to the information in question outweighs the privacy interests of the person who is affected. This balancing test is vague, but it is hugely more protective of privacy interests than American law, which nearly always prevents people from winning anything from search engines and publishers who have spread personal information about them far and wide" (slate.me/1rotmL4).

A different Guardian article says, "The ruling makes clear that a search engine such as Google has to take responsibility as a 'data controller' for the content that it links to and may be required to purge its results even if the material was previously published legally. Data protection lawyers said the ruling meant that..."
Global Efforts to Redefine Privacy in the Age of Big Data
< continued from page 35

Google could no longer be regarded legally as a "neutral intermediary" (bit.ly/SjHenl). Harvard's Jonathan Zittrain believes that the decision, by itself, won't affect practices here in the U.S. "We have a much stronger track record of first, not blaming intermediaries so much for that which they index. And we have the First Amendment." However, others see a parallel with consumer protection laws which, for example, require American credit bureaus to delete credit report information after 7 or 10 years as a form of consumer protection. An editorial in The Boston Globe says, "In essence, Costa [the defendant in the EU case] was asking for the same thing from Google, which has become a de facto background-check service" (bit.ly/1hFphpY).

Brazil Passes Landmark Internet Privacy Law
On April 24, Brazil passed an expansive internet privacy law that holds "American web companies subject to Brazilian law in cases involving domestic users, and includes a net neutrality provision that bars internet providers from charging more for data-heavy services. Known as the Marco Civil da Internet, the law also establishes limits on the metadata that can be collected on Brazilian users and clears service providers of liability for content published by its customers, though it does require companies to remove content under court orders" (bit.ly/RKGOAX).

The law asserts that "Brazilian law and the rights to privacy, protection of personal data, and confidentiality of private communications and records must apply to any operation involving the collection, storage, treatment and custody of records, personal data, or personal communications by connecting providers and Internet applications wherein at least one of these acts occur in the national territory. This applies to data collected in the national territory and to the content of communications, provided that at least one of the terminals involved is located in Brazil. These provisions are applicable even if the activities are performed by a company domiciled abroad, provided that the company offers services to the Brazilian public or at least one member of the company's economic group is established in Brazil" (loc.gov/lawweb/servlet/lloc_news?disp3_1205403949_text).

Timothy Berners-Lee praises the legislation as reflecting "the Internet as it should be: an open, neutral and decentralized network, in which users are the engine for collaboration and innovation. Commendably, the Bill has among its foundations the guarantee of human rights such as privacy, of citizenship and the preservation of the diversity and the social purpose of the web" (webfoundation.org/2014/03/marco-civil-statement-of-support-from-sir-tim-berners-lee).

"As more and more countries follow the EU and Brazil's lead," opponent Eli Sugarman writes in Forbes, "Internet companies will have to navigate an increasingly bewildering web of conflicting Internet rules. Technology investment may flee some jurisdictions as administrative burdens increase; this is especially likely in smaller markets where compliance costs are more difficult to justify" (onforbes.es/IoRhbc).

Streaming Video in Public Libraries < continued from page 1

of collections strategy. The two most popular streaming video lending services, OverDrive and hoopla, are compatible with multiple platforms—PCs, Macs, and Apple and Android devices. OverDrive (company.overdrive.com) launched its streaming video program in November 2013 to complement its catalog of ebooks, audiobooks, music, and Windows-only downloadable videos. hoopla (hoopladigital.com) has offered audiobooks, music, and streaming videos since January 2013 and added ebook lending in May 2014.

Los Angeles Public Library (LA-PL) served as a beta tester for hoopla and then as a pilot library for OverDrive. Peggy Murphy, collection services manager, says the library is a longtime satisfied customer of Midwest Tape (which owns hoopla), and she was a fan of hoopla from the start because of its reporting functionality and "good front end and back end on their product." hoopla provided merchandise that LAPL could give to patrons as advertising: bookmarks, coasters, posters, etc., and it hosted a training day to familiarize staff with the service.

Sandra Fernandez, manager of public relations at Houston Public Library (HPL), has also had a good experience with hoopla since signing up in December 2013. "I implement for customers has been amazingly simple," she says. "I really was prepared when we first launched it to get numerous emails about issues, and I've only gotten very few." Like at LAPL, hoopla helped HPL with marketing and provided training.

LA-PL has been an OverDrive customer since around 2005, and "they've also been a very good company for us," says Murphy. Another longtime OverDrive customer, Phoenix Public Library (PPL), has gotten its ebooks and audiobooks from the service for...