Abuse and Misuse of Personal Information

A Report on Issues and Trends in Privacy

By John Stephenson

ALEC American Legislative Exchange Council

LIMITED GOVERNMENT • FREE MARKETS • FEDERALISM

alec.org

American Legislative Exchange Council

Executive Summary

Advances in technology provide a number of useful products and services that can either enhance or threaten personal privacy, depending on how these products or services are used and for what purpose. These goods raise serious concerns about privacy, which leaves policymakers looking for solutions, especially in the context of online privacy and biometric identification. In an effort to craft solutions to privacy concerns, experts argue that policymakers must exercise caution. Rushed and unconsidered solutions run the risk of limiting consumers and becoming unworkable.

**This report has been researched and published in response to requests by public sector members of the American Legislative Exchange Council and direction by the Communications and Technology Task Force. The author intends for this report to be used as a resource concerning the topics discussed herein. The conclusions in this report reflect the research and views of the author and, therefore, should not be construed as an endorsement of any particular legislation or policy by the Task Force, the Exchange Council, its advisors, or its members.*

INTRODUCTION

Recent stories about abuse and misuse of personal information are driving policymakers to explore the issue and possible responses. When policymakers hear stories about consumers being tracked online and companies and governments collecting biometric information for various purposes, they feel compelled to act. But in the desire to act, policymakers are asking a number of questions about the issues at stake, the technologies at work, the uses for the information collected, and the appropriate responses. Policymakers are quickly learning that addressing the potential for abuse and misuse of personal information is neither easy nor simple. Furthermore, policymakers are realizing that crafting the appropriate policy to respond will require care.

THE CENTRAL QUESTION IS PRIVACY

The central question regarding the abuse and misuse of personal information is: How do we protect our privacy? It is a question easier asked than answered.

"What we once considered private information, such as a birth date or a family photo, is now information we make available to the entire world via the Internet."

Privacy is a vague concept that means many different things to different people. Merriam-Webster's Dictionary defines privacy as "the quality or state of being apart from company or observation." But even this definition leaves out several attributes of privacy. Privacy involves personal information and exercising control over it. Privacy also involves an individual's relationships with others. In recognition of these attributes, Jim Harper of the Cato Institute defines privacy as "the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values."[i] Examples of experiences in exercising privacy show that privacy is inherently subjective.

Many consider privacy a fundamental right, similar to the right to free speech and an important value that must be protected at all costs. However, the United States Constitution does not explicitly mention a right to privacy. Scholars trace the concept of a right to privacy to "the right to be left alone" described in a law review article by Samuel Warren and Louis Brandeis.[ii]

Privacy is also a concept that is constantly evolving due to new technologies and changing social values. What we once considered private information, such as a birth date or a family photo, is now information we readily and freely share, or even make available to the entire world via the Internet. As of April 2012, 900 million people belonged to the social network Facebook.[iii]

Another complication to thinking about privacy is a number of concepts, such as harms, sensitive data, and consent, all of which are understood differently by different people and subject to fierce debate in the legal, political, and policy communities. Additionally, these concepts continue to evolve. Further complicating privacy are what some scholars call a "techno panic," a moral panic that "centers around

societal fears about a specific contemporary technology (or technological activity) instead of merely the content flowing over that technology or medium."[iv] Nevertheless, there is no question that there are people who sincerely want the ability to carve out a zone of privacy for themselves where they aren't assessed, monitored, and recorded by the government or a private entity even if there are negative consequences resulting from such a decision.

"Many of the products and services consumers use on the Internet are free of charge. But these goods are not truly free in an economic sense."

The economics of the Internet also presents a complication for privacy. Many of the products and services consumers use on the Internet are free of charge. In fact, these freely available goods are what have contributed to the Internet's spectacular growth in use and prevalence since the advent of the World Wide Web in the 1990s. But these goods are not truly free in an economic sense. Rather, they are paid for by advertising to consumers. Most websites use some form of this business model. Collection of personal information can be performed to enable better targeting for advertising, which makes the advertising more valuable.[v]

Moreover, the economics of the Internet encourages people to share personal information. People often must share information (i.e. name, age, date of birth, e-mail address, ZIP code, etc.) with companies and each other to use free services. Many Internet-based services such as social networks, photo-sharing websites, and local directory services like Yelp are also specifically designed to encourage the sharing of information with others.

Technology also contributes to the sharing of information phenomena. The advent of tools like faster microprocessors, networked storage, and wireless broadband have all created the capacity to rapidly share vast amounts of data from anywhere to everywhere in the world. The amount of information being created is staggering: every 60 seconds, it is estimated that over 6,600 photos will be uploaded to Flickr; Google serves more than 694,445 queries; over 1,200 new ads will be created on Craigslist; and 695,000 status updates, 79,364 wall posts and 510,040 comments are published on the social networking site Facebook.[vi]

Recently, consumers have expressed concerns about the use of targeted advertising and data collection by certain popular Internet companies. The Pew Internet & American Life Project reported that 68 percent of those it surveyed were not OK with targeted advertising because "they don't want their activities tracked and analyzed."[vii] Ironically, the speed with which the Internet has grown and become an integral part of society is precisely what sparked and fueled concerns about privacy. Given the nature of the Internet, there is an argument that information put on the Internet is not meant to be kept private. The counterargument is that the nature of the Internet means that some people cannot easily avoid sharing information about themselves and are in need of policies to protect their personal information from misuse and abuse.

APPROACHES TO PRIVACY: THE UNITED STATES VERSUS THE EUROPEAN UNION

Policymakers around the world have been debating responses to concerns about privacy since the beginning of the Internet. During that time, there have been several responses to address consumer concerns from both industry and government. It's possible to categorize the response approaches seen thus far by the geographic regions from which they come, namely the European Union approach and the United States approach.

> *"In the United States, privacy is a right that has developed out of the constitutional rights to due process and no unreasonable searches and seizures."*

Europe views privacy as a fundamental right. European countries' laws and regulations are broad, top-down directives that aim to protect privacy against private entities. An example of this approach is the European Union's Data Protection Directive, which defines personal data, imposes obligations on entities that control data, and creates several rights for recourse by individuals who may be concerned about the use of their data.[viii]

In the United States, privacy is not viewed as a fundamental right. Rather, it is a right that has developed out of the constitutional rights to due process and no unreasonable searches and seizures. Traditionally, Americans' concerns about privacy arose from fears of government access to personal information. Only during more recent times has the focus of concerns been on companies' access to personal information of consumers and what the companies might do with it after collection, such as turning it over to the government.[ix]

> *"Whether law enforcement or self-regulation, the focus of these actions has been largely on ensuring consumers have sufficient notice and choice when it comes to making decisions about privacy."*

When it comes to privacy law, the U.S. and state governments generally use laws and regulations based on tort and common law theories aimed at specific parts of the government or sectors of the economy. The modern day U.S. approach to privacy dates back to the 1970s when the federal government, in response to concerns about the sharing of health data, promulgated the Fair Information Practice Principles, which are a set of internationally-recognized practices for addressing the privacy of individuals.[x]

Most U.S. privacy laws are federal statutes reflecting the inherently interstate nature of information flows. However, states have not shied away from enacting privacy laws to address their own needs or the concerns of constituents. Other examples of the U.S. approach to privacy include the Privacy Act of 1974 (regulating government collection and dissemination of personal information), the Health Insurance Portability and Accountability Act (regulating the use of health records by covered providers), and the California Online Privacy Protection Act (requiring commercial websites collecting information from residents of California to conspicuously post online and comply with a privacy policy).

Agencies like the U.S. Federal Trade Commission and state attorneys general have engaged in targeted enforcement against companies and other entities believed to be in violation of privacy laws. Additionally, in the U.S. there is a clear preference for industry self-regulation through various bodies and mechanisms, such as codes of conduct. Whether law enforcement or self-regulation, the focus of these actions has been largely on ensuring consumers have sufficient notice and choice when it comes to making decisions about privacy.[xi]

CONCERNS ABOUT BIOMETRICS

Concerns regarding privacy and what to do about it are not limited to the online consumer sphere. New fronts are opening with the advent of new technologies that use more or new kinds of personal information to offer new products and services. One recent example of this phenomenon is biometric identification.

Technically, biometrics is simply the measurement of living things. Biometric identification is the measurement of identifiers from living (and formerly living) things to distinguish them from one another.[xii] More commonly, biometric identification is the automated process of identification of a person based on that person's unique physical or behavioral characteristics. The basic process for biometric identification today is as follows: personal information (like fingerprints) is measured by a sensor machine and recorded. In a fingerprint analysis, for example, the sensor measures the distances and angles of the endings, ridges, and bifurcations that comprise the fingerprint. The sensor converts the measurements into a digital description, and a computer compares it against another description (or set of descriptions) to find a match.

"Many applications that use biometric identification protect privacy by screening out those attempting to commit identity fraud by posing as another individual."

With advances in technology, it is becoming possible to take new measurements with increasingly greater accuracy. A combination of faster microprocessors and better sensors can distinguish physical and behavioral characteristics that are imperceptible to the senses and previously only possible to identify through advanced science. Facial recognition technologies can employ methods such as geometric, photometric, and skin texture mapping to find matches with great speed and accuracy. For example, in 2010, the National Institute of Standards and Technology tested various facial recognition systems and found that the best algorithm correctly recognized 92% of unknown individuals from a database of 1.6 million criminal records.[xiii]

Verifying identity is an important part of social interactions whether in commerce or public safety settings. Humans need to know with whom they are interacting in order to establish the level of trust necessary for completing a deal or sharing a secret. Such is why applications for biometrics include criminal background checks, controlling access to secure facilities, protection of sensitive information, and verifying eligibility for taxpayer-financed benefits. It can be stated that many applications using biometric identification protect privacy by limiting access to only those individuals who are eligible for a privi-

lege or benefit and screening out those attempting to commit identity fraud by posing as another individual.

Although biometric identification is not new, the practice is becoming more widespread due to a number of factors. Advances in technology are making biometric identification faster and more accurate. Those same technological advances are also making the process cheaper to use. It is now possible for the average consumer to buy electronic devices using biometric identification processes in a number of ways, such as fingerprint sensors for accessing personal computers or information systems.

Widespread use has also contributed to the adoption of more standards for biometric identification. The standardization and reduction in costs has led consumers, businesses, and governments to adopt biometric identification methods for security and privacy applications. Industry groups predict that use of biometrics will continue to grow as a result of these factors, the ubiquity of advanced electronic devices, and ongoing consumer and business concerns about privacy and security.[xiv]

There are real benefits to using biometric identification. Biometrics can provide highly assured verification of identify. Physical characteristics like fingerprints and irises cannot easily be copied. Biometric information cannot be forgotten like a password or a PIN code. Additionally, machine-readable biometrics can quickly verify that an individual is the person he claims to be or identify who a person is by searching a repository of biometric identifiers. Machines are also not subject to the same pressures or shortcomings as humans. Therefore, biometrics provides a greater degree of security for data, which helps ensure privacy.

Biometrics is not a panacea to privacy and security. In fact, it presents its own privacy challenges.

Biometric identification also creates opportunities for new commercial applications. For example, social networks like Facebook and photo-sharing services like Flickr offer users biometric identification to tag friends in photos they share online to improve and increase the amount of searching and social interactions. Some companies and advertisers are experimenting with digital signage, which are basically dynamic billboards that display advertising based on facial recognition of the consumer nearby. For example, a digital sign at the entrance of a retail clothing store scans the faces of customers who enter the store. The sign will display an advertisement for a new pair of women's shoes as a woman walks by the sign, then switch to an advertisement for a pair of men's shoes as a man walks by. The advertisement displayed could change based on the marketer's target audience.

However, biometrics is not a panacea to privacy and security. In fact, it presents its own privacy challenges. One major problem is that humans' physical characteristics can change over time. For example, natural changes like aging, common ailments like dry skin, and injuries can make fingerprints and other physical characteristics difficult to read.[xv] Furthermore, there is a real risk of identity theft if the stored sample of biometric information, which like most data can be stored indefinitely and copied multiple times, is lost or stolen.[xvi] Advances in technology may also provide criminals with new methods to steal biometric information and use it to gain access to sensitive information. Additionally, biometric

information, such as DNA, could be used to reveal previously unknown details about a person's health such as susceptibility to disease. With more data available, there is a greater risk to privacy.

That said, the use of biometrics is in an early stage of development for non-government commercial applications and continues to evolve. Technological improvements increase the accuracy of measurements. At the same time, there is more information to exploit for good and bad purposes in ways we cannot anticipate. The potential benefits and shortcomings of biometrics are yet to be determined. The indeterminate consequences of technology make crafting policy concerning biometric identification a real challenge.

SOLUTIONS FOR POLICYMAKERS*

We must use great care to craft privacy policies that guard against the drawbacks without jeopardizing the benefits of new technologies. If history is any guide, rushed solutions typically turn out to be unworkable and costly complications. Narrow solutions also present workability and cost problems.

"If history is any guide, rushed solutions typically turn out to be unworkable and costly complications."

Consider the example of the Do Not Track (DNT) mechanism. Basically, DNT means a mechanism by which websites honor a header indicating the user requests not to be tracked for advertising or other purposes. However, no common standards for DNT currently exist and attempts to negotiate such standards have been moving slowly. Research has also found that restrictions on the ability to advertise have real costs. After the EU enacted the Privacy Directive, "advertising effectiveness decreased by around 65% in Europe." With the decline in ad effectiveness, "this may change the number and types of businesses sustained by the advertising-supporting Internet."[xvii]

The type of solution policymakers choose to employ can also add to policymakers' challenges. As suggested earlier, the inherently interstate nature of information flows make effective state laws a challenge. Additionally, the marketplace tends to prefer one set of rules to establish standards and keep compliance costs low. However, some state consumer protection statutes and state enforcement mechanisms (i.e. state attorneys general) have proven to be very effective at enforcing the law in a variety of circumstances. For example, 47 states have adopted data breach notification laws to guard against identity theft.[xviii]

Consumers must feel that they can trust a technology with their information or else they won't use it. Whether it is online activity or biometric identification, we do not have to sacrifice privacy to enjoy new products and services. Real privacy solutions are possible, but only if they reflect the reality of how information is collected and used.

Not all biometric identification applications are equal. The gathering of biometric information does not, in every context, result in individual identification and raise privacy or security concerns. In some cases, biometric information is gathered in the aggregate for research purposes but is not retained. For

*These proposals have not been formally endorsed by the Exchange Council. They are discussed here to present a range of perspectives currently being discussed within the policy community. For a list of some privacy principles endorsed by the Exchange Council, see the ALEC Statement of Principles for Online Consumer Privacy (Adopted Oct. 2012).

> *"Whether it is online activity or biometric identification, we do not have to sacrifice privacy to enjoy new products and services."*

example, facial recognition can be used to indiscriminately count the number of adult males who enter a store during a sale. It is when biometric information is collected and used to identify an individual that privacy concerns are raised.

Current federal law only punishes the use of biometric information for fraud and identity theft.[xix] Additionally, the Privacy Act and guidelines issued by the U.S. Office of Management and Budget cover and restrict the use of biometric information held by federal agencies. There are also federal and some state laws that prohibit secret videotaping and photographing, but these are very narrowly tailored laws.

With two exceptions, state law says very little about regulating the collection and use of biometric information. Texas prohibits the capture of biometric identifiers for commercial purposes without notifying the individual and obtaining the individual's consent to capture the biometric identifier.[xx] The Illinois Biometric Information Privacy Act regulates the collection, use, and storage of biometric information and requires protection of that information by private entities. There is, however, an exception if the disclosure is required by law or pursuant to a valid warrant or subpoena.[xxi]

To address these concerns, policymakers have proposed a variety of legislative and regulatory changes at the federal and state levels. In the 112th Congress, Senators John Kerry and John McCain introduced the Commercial Privacy Bill of Rights Act of 2011, a comprehensive baseline privacy bill that would have limited data collection and allowed users to opt out of data collection for behavioral advertising, among other things. Other bills introduced in the last Congress focused on specific issues such as an expansion of the federal Children's Online Privacy Act, restrictions on geolocation tracking, and a requirement for a DNT mechanism. In California, Senate Bill 761 would have required a DNT mechanism for California residents. However, none of these bills received a vote in a full legislative chamber.

The reaction to abuse and misuse of personal information through biometric identification has been similar to that surrounding online privacy, for states have proposed specific legislation to target the issue. In Alaska, for example, a bill introduced in the 2012 legislative session (Senate Bill 98) would limit the collection and use of biometrics without express consent. Proponents argue that these restrictions are necessary to prevent the exploitation of biometric information for profit.[xxii] Opponents criticize these restrictions for being overly broad and unworkable.[xxiii]

The International Biometrics & Identification Association (IBIA), an industry trade group, acknowledges that the public may perceive biometric identification as both a threat to personal privacy and a way to safeguard privacy. But IBIA also believes that there is more of a concern over the use of biometric data than with the technology used to collect information. Therefore, IBIA recommends the development of policies to protect the privacy of biometric data rather than preemptively regulate the technology.[xxiv]

To that end, IBIA recommends biometric identifiers be treated as personally identifiable information (PII). Like PII, IBIA asserts that biometric information should be safeguarded to ensure it is not misused or compromised. Biometric information shouldn't be distributed or shared without informed consent or authority of law. Additionally, IBIA recommends private entities take any necessary steps to secure biometric data, limit the use of data beyond its intended purpose, and inform consumers how data is collected and used. IBIA also recommends that public entities, such as government agencies and legislatures, develop clear legal guidance on standards that define and limit the conditions under which public institutions or agencies may acquire, access, store, share and use biometric data and other PII.

However, with regard to legislation, IBIA cautions that any proposed laws to limit the use of biometrics should be narrow and not overly broad. Legislation, IBIA emphasizes, should not inhibit or unduly burden legitimate applications of biometric technology because doing so would present an obstacle to its beneficial use.

The Center for Democracy and Technology (CDT), an advocacy group that has considered policy for facial-recognition technologies, argues that a mix of government regulation, industry self-regulation, and privacy technologies are needed to give consumers greater control over their information without limiting the technologies and retarding innovation.[xxv] CDT notes that within the past two years industry groups such as the Digital Signage Federation have adopted privacy standards on facial recognition modeled on the widely-used Fair Information Practice Principles and include provisions governing notice, consent, and use of biometric information. CDT supports these efforts and calls on industry to continue work on this front, as well as develop new tools to enhance privacy when regulations or company policies are not enough.

But CDT also notes that it does not believe self-regulation without appropriate incentives and enforcement mechanisms is sufficient to protect consumer privacy.[xxvi] CDT policy experts have stated their view that it is important to frame privacy rules as allowing individuals to make informed market choices about what is best for their personal privacy. In particular, there is concern that current law actually disincentivizes disclosure about privacy practices. Therefore, CDT advocates for a strong, baseline privacy law by Congress. This baseline law, CDT argues, should cover biometrics and transparently provide consumers details about biometric information collection and use, and include for consumers a measure of control over whether they participate in biometric identification. CDT also believes that baseline consumer privacy legislation should establish a safe harbor program in which companies that adhere to enforceable industry self-regulatory privacy codes enjoy specified incentives such as exemption from liability.[xxvii] There should also be special considerations for vulnerable populations, such as children.

CDT recognizes that its approach also comes fraught with issues. What to do about publicly available information and the regulation of individual use of technology present two very difficult questions for policymakers to address. These questions also raise First Amendment concerns. To help allay some of these issues, CDT does not support laws that target discrete technologies or economic sectors, arguing

that these laws only add to the currently fragmented body of privacy law.[xxviii] Rules derived from these fragmented laws will only confuse businesses and consumers, serving no one in the long run.

Rather than a problematic regulatory approach to biometrics, Jim Harper of the Cato Institute argues for addressing concerns about biometrics through contract and tort laws.[xxix] If biometrics are collected based on promised limits for how they are used and stored, for example, states should ensure that their laws create causes of action for violations of those promises. States could also amend their jurisdictional statutes and statutes of limitations accordingly to protect citizens from out-of-state biometric collectors. To protect against government privacy invasion, Harper suggests that states could establish that the U.S. Supreme Court's Third Party doctrine (holding that information a person shares with another is not subject to protection under the Fourth Amendment) does not apply in state law.

It is also worth noting that some companies have adjusted their business practices to address concerns about privacy. For example, Google's Picasa (web-based photo album) lets the user tag photos of friends rather than doing it automatically.[xxx] Businesses such as Apple and IBM are also incorporating "privacy by design" (privacy and data protection through the life cycle of technologies) in their products and services. Privacy by design is a concept that has been endorsed by the U.S. Federal Trade Commission as the best way to address privacy concerns before they arise.[xxxi]

Adam Thierer of the Mercatus Center argues in favor of a resiliency (coping) rather than an anticipatory (prevention) approach to privacy, given the changing nature of technology and how we value privacy. To that end, he proposes a "3-E Solution" to privacy problems: education, empowerment, and enforcement.[xxxii] First, Thierer favors education about privacy issues and solutions at all levels through awareness campaigns undertaken by government, industry, and advocates. Additionally, he supports a push for better transparency for notice and privacy promises.

"Only through careful consideration will policymakers be able to protect their constituents and innovation."

Second, Thierer wants to see help for users who want to help themselves. This means encouraging the development of tools like web browser plug-ins that block certain undesirable program scripts or advertising.[xxxiii] Further, he believes industry should be encouraged to collaborate on privacy programs to share best practices. Together, these efforts encourage corporate and personal responsibility.

Finally, Thierer believes that it is necessary to hold accountable entities that break their promises. However, he does not believe new law or regulation is necessary to do this. Thierer argues that under existing federal and state law (e.g. Section 5 of the Federal Trade Commission Act and state consumer protection law), the government has sufficient authority to take action against entities that break promises to users.[xxxiv] But if there must be additional law, he reasons it should focus on targeted regulation of sensitive data (i.e. health records), data breaches, and transparency.

CONCLUSION

Policymakers will continue to hear from constituents and activists concerned about the abuse and misuse of information. Concerns about online privacy and biometric identification may even increase in scale and scope as uses for biometric data multiply and the technology improves. But the lesson for policymakers from their experiences thus far appear to be that the issues and technologies evolve, and so policymakers must exercise great care in crafting their responses. Only through careful consideration will policymakers be able to protect their constituents and innovation.

---

[i] Harper, Jim. "Understanding Privacy – and the Real Threats to it." Cato Institute Policy Analysis No. 520 4 Aug. 2004.

[ii] Samuel Warren & Louis Brandeis. The Right to Privacy, 4 Harvard L.R. 193 (1890).

[iii] Goldman, David "Facebook tops 900 Million Users," CNN Money, 23 Apr 2012. Web 04 Jan 2013.

[iv] "Ongoing Series: Moral Panics/Techno Panics." Tech Liberation Front. n.d. 03 Jan. 2013.

[v] Beales, Howard. "The Value of Behavioral Advertising." Network Advertising Initiative n.d. Web. 14 Jan. 2013

[vi] Golijan, Rosa. "What Happens on the Internet Every 60 Seconds." NBC News. n.d. Web 03 Jan. 2013.

[vii] Evangelista, Benny. "Internet Privacy a growing concern, Pew finds." *The San Francisco Chronicle* 10 Mar. 2012: Online.

[viii] "E.U. Data Protection Directive." Electronic Privacy Information Center. n.d. Web. 02 Jan. 2013.

[ix] Szoka, "Protecting Privacy and Preserving Innovation in the States."

[x] Gellman, Bob. "Fair Information Practices: A Basic History." Bob Gellman 12 Nov. 2012. Web. 03 Jan. 2013

[xi] Thierer, Adam. "Online Consumer Privacy: Current Trends." 2011 Exchange Council States and Nation Policy Summit. Westin Kierland Resort, Phoenix, AZ 01 Dec. 2011. Telecommunications and Information Technology Task Force Presentation.

[xii] Harper, Jim. "Testimony on Alaska Senate Bill 98." Alaska House Health and Social Services Committee Meeting. 27 Mar 2012.

[xiii] Griger, Harley. "Seeing is ID'ing: Facial Recognition and Privacy." Center for Democracy and Technology. 22. Jan 2012. Web. 31 Dec. 2012

[xiv] Hamilton, Walter. "Biometric Identification: Technologies and Policy Considerations." 2011 ALEC States and Nation Policy Summit. Westin Kierland Resort, Phoenix, AZ 01 Dec. 2011. Telecommunications and Information Technology Task Force Presentation.

[xv] Raven, Kathleen. "Dermatitis can lead to fingerprint ID failures." *Chicago Tribune*. 28 Dec. 2012.

[xvi] Harper. "Testimony on Alaska Senate Bill 98."

[xvii] Goldfarb, Avi and Tucker, Catherine, Privacy Regulation and Online Advertising (August 4, 2010). Available at SSRN: http://ssrn.com/abstract=1600259 or http://dx.doi.org/10.2139/ssrn.1600259

[xviii] Brookman, Justin. "Protecting Privacy and Preserving Innovation in the States." 2012 Exchange Council States and Nation Policy Summit. Grand Hyatt Washington, Washington, DC. 28 Nov. 2012. Consumer Protection, Critical Infrastructure, and Security Technologies Subcommittee Presentation.

[xix] Griger. "Seeing is ID'ing: Facial Recognition and Privacy."

[xx] Tex. Bus. & Com. Code Ann. § 503.001(a)-(b).

[xxi] 740 ILCS 14

[xxii] Hubbel, Lora. "Misuse and Abuse of Personal Information." 2012 Exchange Council Annual Meeting. Grand America Hotel, Salt Lake City, UT. 25 Jul. 2012. Consumer Protection, Critical Infrastructure, and Security Technologies Subcommittee Presentation.

[xxiii] Harper. "Testimony on Alaska Senate Bill 98."

[xxiv] Hamilton. "Biometric Identification: Technologies and Policy Considerations."

[xxv] Brookman. "Protecting Privacy and Preserving Innovation in the States."

[xxvi] Griger. "Seeing is ID'ing: Facial Recognition and Privacy."

[xxvii] Id.

[xxviii] Id.

[xxix] Harper, Jim. "Misuse and Abuse of Personal Information." 2012 Exchange Council Annual Meeting. Grand America Hotel, Salt Lake City, UT. 25 Jul. 2012. Consumer Protection, Critical Infrastructure, and Security Technologies Subcommittee Presentation.

[xxx] Griger. "Seeing is ID'ing: Facial Recognition and Privacy."

[xxxi] "Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies." Federal Trade Commission 22 Oct. 2012. Web. 03 Jan. 2013

[xxxii] Thierer. "Online Consumer Privacy: Current Trends."

[xxxiii] Id.

[xxxiv] Id.

The mission of the **American Legislative Exchange Council** is to advance principles of free markets, limited government, and federalism through developing and promoting sound public policies in a nonpartisan partnership of nearly one-third of America's state legislators and 300 members of the private sector.

The **Communications and Technology Task Force** is the premier forum for state communications and technology policy. To guide policymakers through the uncharted waters of the 21st Century economy, the Task Force brings together reformist state legislators, leading industry representatives, and public policy experts. Working together, the Task Force seeks to develop model state public policy that will promote economic growth, freedom of technology, and innovation for all.

John Stephenson
Director, Communications and Technology Task Force
Email: jstephenson@alec.org
Office: 202-742-8524