Luther Martin


Your organization needs to comply with privacy regulations. Your board of directors knows the business needs to protect sensitive information as it moves among business partners, mobile users and your enterprise. Yet security technologies such as encryption are far too complex and far too difficult to deploy on a broad scale.

Actually, that is no longer the case. Leveraging identity-based encryption (IBE) is far easier and more scalable than traditional encryption technologies.

On September 7, 2006, the five major credit card companies announced the formation of a new organization to improve and implement the PCI standard, marking the first time that the five major brands (American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International) have agreed to a single, shared framework. The new group, known as the Payment Card International Security Standards Council, took its first action by issuing PCI 1.1, an updated version of PCI DSS.


The PCI Data Security Standard has prompted relatively little action by merchants. Visa recently

See, PCI Data Security Standard, page 3

Enabling Data-Centric Security

By Luther Martin

On September 7, 2006, the five major credit card companies announced the formation of a new organization to improve and implement the PCI standard, marking the first time that the five major brands (American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International) have agreed to a single, shared framework. The new group, known as the Payment Card International Security Standards Council, took its first action by issuing PCI 1.1, an updated version of PCI DSS.


The PCI Data Security Standard has prompted relatively little action by merchants. Visa recently

See, PCI Data Security Standard, page 3

This Month

J. Trevor Hughes on the Inaugural European Delegate Tour ............Page 2
India and Outsourcing ......................Page 7
Ask the Privacy Expert ....................Page 10
Privacy Classifieds .........................Page 11
Regulator Chat .............................Page 12
IAPP in the News .........................Page 14
Update: Statutory Review of PIPEDA Page 15
Certification Graduates .................Page 17
Privacy News .............................Page 18
Calendar of Events ......................Page 20
Notes from the Executive Director

As part of the IAPP’s international commitment, we are proud to announce the launch of our inaugural European delegate tour. While details are still in the works, the delegate tour is a unique opportunity for IAPP members to participate in a series of special events in London, Paris and Berlin. Scheduled for June, the tour is expected to give privacy pros an opportunity to compare notes with our European colleagues in each city during KnowledgeNet meetings, workshops with data protection authorities and networking opportunities.

The first European delegate tour would not be possible without the generous support of Microsoft and Ernst & Young. The IAPP is excited about this tour as we continue our efforts to broaden our mission to promote the privacy profession globally. We eagerly look forward to learning from and collaborating with international privacy pros.

And now for the good news! IAPP members will have the opportunity to attend these exciting events — at no additional cost. All we ask is that members cover the cost of their travel expenses and hotel stay. The IAPP will provide all the programming, including networking meetings and workshops, in each city. This spectacular networking opportunity has to be one of the best values — and we are thrilled to offer our members the chance to take part in what is sure to be a memorable tour. Members who are interested in participating in this unique privacy programming are encouraged to contact Kimberly MacNeill, the IAPP’s Member Networking Manager, at kim@privacyassociation.org. Please note there may be some space limitations.

Let me take a moment to also update you on another IAPP global privacy effort. Peter Kosmala, the IAPP’s Assistant Director, recently returned from a week in Singapore, where he spoke at an online privacy conference co-sponsored by the IAPP and LexisNexis, and met with privacy leaders across the private and public sectors in Singapore. These included KK Lim, CIPP Chief Privacy Officer-Asia Pacific, IMS Health; Lawrence Tan, CIPP/G, Senior Consultant, IDA-Infocomm Development Authority of Singapore; Jeff Bullwinkel, Director of Corporate Affairs-Asia Pacific, Microsoft, Singapore; and Wei Choo Hua, Corporate Attorney, Microsoft, Singapore, among many others.

With more than 6,000 multinational corporations based in the country, 106,000 working IT professionals, and a growing community of privacy professionals, Singapore is a hotbed for innovation and ripe this year for legislative action in the data protection arena. Peter’s trip is a follow-up to the IAPP’s Asia Pacific Tour last year, when we took our signature privacy networking program on the road, holding KnowledgeNet meetings in Sydney, Singapore and Tokyo. While it is unclear at this juncture what specific developments are likely from the IAPP’s collaboration with privacy leaders in Singapore, the IAPP definitely will continue our activity and coordination in the Asia Pacific Region in the months ahead — so stay tuned!

On the domestic front, look next month for coverage of the IAPP Privacy Summit 07 in Washington, D.C., an enormously successful conference lauded by privacy professionals from near and far.

J. Trevor Hughes, CIPP
Executive Director, IAPP
estimated that only 22 percent of the largest merchants (those that handle more than 6 million credit card transactions per year) are PCI-compliant today. But it expected that number to climb dramatically by the end of 2006. Visa also has estimated that 72 percent of the largest merchants have conducted an initial PCI audit, identified their deficiencies and have a remediation plan in place to achieve full compliance.

Merchants ignoring the growing adoption of the PCI DSS do so at their peril because the penalties for noncompliance are severe. Noncompliant merchants and payment processors can face as much as $500,000 in fines per incident if cardholder data is compromised. Visa has reported that it imposed $4.6 million in fines against banks in 2006, up from $3.4 million in 2005. Even more devastating than fines, credit card companies also may revoke the right of a merchant to process credit card transactions, a virtual death sentence for many businesses.

Carrots and Sticks
On December 12, 2006, Visa announced a new program, known as the “Visa PCI Compliance Acceleration Program,” which seeks to create financial incentives to encourage PCI compliance. Under the program, Visa has committed $20 million to offer financial incentives to banks that process credit card transactions if they can demonstrate that the merchants they deal with are PCI-compliant. A Visa spokesperson has stated that the new program is intended to supplement the “stick” of noncompliance penalties with a “carrot” in the form of financial incentives.

It appears that credit card associations may no longer be the only parties seeking to compel compliance by merchants with PCI DSS standards. In January 2007, the director of the Massachusetts Office of Consumer Affairs and Business Regulation announced plans to call on merchants to begin disclosing the extent to which they comply with the PCI DSS. In February 2007, a class action claim filed in Massachusetts federal district court charged that TJX, Inc. failed to adhere to PCI standards.

PCI’s Three-Tiered Approach
The PCI DSS applies to three tiers of entities: the merchant, the acquiring bank and the credit card associations that are members of the PCI Security Standards Council. Merchants are the first tier because they are on the “front lines” of credit card transactions. A merchant, either through a physical store or a Web site, accepts credit card payments from the consumer. The PCI Data Security Standard assumes that merchants are in the best position to safeguard credit card information because they are the point of contact with the consumer. As a result, merchants bear the brunt of the standard’s compliance obligations.

The second level is the “acquiring bank” or “acquirer.” A merchant that processes credit card transactions must have a relationship with an acquiring bank that processes the transaction. The merchant contacts the acquirer to confirm that the consumer has sufficient funds. The third tier involves the “cardholder” or “consumer,” who is the point of contact for the acquiring bank. The acquiring bank processes the transaction and pays the merchant.

See, PCI Data Security Standard, page 4

“Merchants ignoring the growing adoption of the PCI DSS do so at their peril because the penalties for noncompliance are severe. Noncompliant merchants and payment processors can face as much as $500,000 in fines per incident if cardholder data is compromised.”
funds in the consumer’s account and authorizes payment.

The credit card associations occupy the third tier. The associations develop PCI standards and impose them upon the acquiring banks, which are responsible for implementation of, and compliance with, those standards. The associations do not have a direct relationship to the merchants, and rely upon the acquiring banks to enforce the PCI requirements with respect to merchants.

Encryption and Compensating Controls

One PCI standard creating headaches for merchants is the requirement of database encryption. A covered entity must render cardholder data unreadable anywhere it is stored by using strong cryptography, such as Triple Data Encryption Standard 128-bit encryption, or other specified methods. It appears that even many large processors of credit card transactions have not yet achieved full PCI compliance due to the time and cost associated with implementing database encryption projects.

The PCI Security Standards Council’s September 2006 update of the standards made this requirement more flexible, providing that if for some reason a company is unable to encrypt cardholder data, “compensating controls” may be employed. The update provides that compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a technical specification of a requirement, but has sufficiently mitigated the associated risk through other controls.

The PCI Security Standards Council has issued a PCI DSS Glossary, which specifies that compensating controls must: (1) Meet the intent and rigor of the original stated PCI DSS requirement; (2) Repel a compromise attempt with similar force; (3) Be “above and beyond” other PCI DSS requirements; and (4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

Clearly, this new flexibility is by no means an easy out for merchants seeking to bypass PCI’s encryption standard or other standards posing implementation difficulties. Merchants that fail to encrypt cardholder data must be prepared to perform a PCI security audit to demonstrate the presence of “compensating controls” and “mitigating circumstances.” It also is becoming apparent that different auditors have different interpretations of what “compensating controls” and “mitigating circumstances” are adequate. Differing interpretations of these critical terms could lead to significant variation in implementation of PCI DSS and “forum shopping” for security auditors who are perceived to have adopted a more lenient (and less costly) reading of the standards.

Penalties for Noncompliance

Although the credit card associations have not been very active thus far in enforcing the PCI Data Standard, the potential consequences of noncompliance are severe. Acquiring banks are responsible for monitoring PCI compliance and reporting noncompliant merchants. An acquiring bank may report a merchant violating PCI to the Terminated Merchant File or MATCH list, which is available to other acquirers. A merchant placed on the MATCH list will have great difficulty in processing credit card transactions, and there is no clear process for a merchant to appeal the determination.

The most substantial penalties may be applied if the credit card association determines that a security breach occurred and, at the time of the breach, the merchant was not PCI-compliant. In such a case, the merchant will be responsible for a full-scale investigation of the breach. After the investigation, the merchant must obtain a PCI compliance certification in order to continue processing credit card transactions. The merchant also may be responsible for any and all charges posted to credit card numbers obtained through the

---

**The Digital Dozen**

The PCI Data Security Standard contains basic security requirements, also known as the “digital dozen.” The Standard requires covered entities to:

- Install and maintain a firewall configuration to protect data;
- Not use vendor-supplied defaults for system passwords and other security parameters;
- Protect stored cardholder data;
- Encrypt transmission of cardholder data and sensitive information across public networks;
- Use and regularly update anti-virus software;
- Develop and maintain secure systems and applications;
- Restrict access to data by business need-to-know;
- Track and monitor all access to network resources and cardholder data;
- Regularly test security systems and processes; and
- Maintain a policy that addresses information security.

Unlike many statutes and regulations that address data security, the PCI DSS includes specific metrics and specifications for each of the requirements. Nevertheless, PCI’s digital dozen generally reflect basic security principles consistent with reasonable best practices.
"Merchants should be proactive and adopt a diligent approach to PCI compliance, as part of an enterprise-wide approach to privacy and security."

The volume of credit card transactions they process annually. Most merchants will fall into merchant levels 2 (between 1 and 6 million transactions), 3 (fewer than 1 million transactions) or 4 (fewer than 20,000 online transactions). Merchants in levels 2, 3 and 4 are permitted to “self-certify” their compliance with the PCI Data Standard, rather than obtaining a PCI audit from an independent vendor. It is relatively easy for a merchant to self-certify and take a lax approach to PCI compliance — but that places the merchant in a very dangerous position if it experiences a security breach involving credit card transactions.

Therefore, merchants should be proactive and adopt a diligent approach to PCI compliance, as part of an enterprise-wide approach to privacy and security. Merchants should not shy away from the more complex aspects of PCI compliance, such as database encryption, establishing a security-oriented hiring policy for staff and contractors, and assigning each person a unique ID for accessing data. In addition, covered entities should amend their contracts with vendors that access cardholder data to include certain PCI-specific provision, such as the right to audit to validate compliance with the PCI standard.

While the PCI Data Standard will undoubtedly continue to evolve, any changes are likely to only facilitate wider adoption of the standard. In short, the PCI Data Standard is rapidly becoming an inescapable fact of life for all merchants that process credit card transactions.

Reece Hirsch is a partner in the San Francisco office of Sonnenschein Nath & Rosenthal LLP specializing in privacy and data security issues. He can be reached at +415.882.5040 or rhirsch@sonnenschein.com.

A version of this article appeared previously in BNA’s Privacy & Security Law Report.
Your Identity, Your Privacy

IBE can use almost anything as a person’s identity, an email, IP or hardware address — as long as it’s unique. Today, more than 5 million users worldwide leverage IBE to encrypt email messages, and for most, their email addresses are their identities.

A big benefit to organizations is that it is also quite easy to include policy information in an IBE key. Instead of encrypting using the identity — “alice@gmail.com,” it’s just as easy to encrypt using the identity “alice@gmail.com&classification=PCI.”

The way to calculate an IBE encryption key is publicly known, and all IBE-enabled applications can do it. Data from existing Identity and Access Management (IAM) systems can define identities, helping increase the return on that investment as IBE is used to solve the problem of managing data privacy.

For decryption to take place using IBE, a user has to be able to authenticate to a key server. The user who requests a key needs to prove he or she are authorized to receive it. If “alice@gmail.com&classification=PCI” is used as an IBE encryption key, for example, a user might have to prove both that he or she owns the email account (alice@gmail.com), and that he or she is entitled access to the PCI information before the key server grants the decryption key.

This ability to implement policy within the keys separates IBE from other encryption technologies. Further, IBE can easily implement the type of complex policies that data privacy regulations require.

Supporting Structured & Unstructured Data

The ease of using IBE to encrypt data is not affected by the level of structure in it. Traditionally, it has been manageable to encrypt a database, a case where the data is highly structured. Encrypting data with less structure, like email, has been more difficult, which has limited the adoption of the technology. Even more challenging has been encrypting unstructured data, like documents and spreadsheets, which can reside anywhere on a network yet still contain sensitive information.

IBE resolves these challenges. Indeed, it makes policy-based encryption very easy to implement by embedding policy in encryption keys and requiring authentication to get the corresponding decryption keys. The same key management platform can be used for all three cases, so IBE can form the basis for an enterprise-wide key management strategy that can extend easily to include new applications.

Clearly, IBE has solved many of the encryption challenges that today’s enterprises face. By embedding policy directly in keys, IBE makes it easy to enforce policy. And by leveraging existing IAM infrastructure to define identities, IBE easily integrates into existing infrastructures.

At long last, encryption will be a key enabling technology that empowers us to ensure data-centric security.

Luther Martin is chief security architect at Palo Alto, CA–based Voltage Security, Inc. (www.voltage.com). He is the author of the IETF draft standards on identity-based encryption algorithms and their use in encrypted email, and is a frequent author in the areas of information security, risk management and project management. His interests include pairing-based cryptography, business applications of information security and risk management. He holds a MS degree from The Johns Hopkins University in Electrical Engineering. He can be reached at martin@voltage.com.
Sagi: Can you describe some of the key differences from a privacy and data protection perspective that are more obvious about doing business in the EU, the U.K. and the U.S. and India? Is there a specific India risk that we should be aware of?

Mark: To start with, if you are looking at the kind of legislative differences and the types of framework that you have, that is not in place in India. You don’t have that kind of safety net. There is no equivalent of the European Union directive on data protection or the U.S. equivalent, the concepts of Safe Harbor. Even in the most recent information technology legislation — which was written in 2000 — the idea of data protection was not included, so there is an immediate difference there in that you don’t have that legal kind of framework around you to start with. That means that the environment is very much one of the private sector. The companies themselves actually have to demonstrate the capability rather than there being a law that they’ve got to adhere to.

The other sort of real major difference in working in an environment such as India is you are going to work in a developing country. You’ve still got quite an extreme policy in some parts of the country, and so what you will actually see is that the corporations have to build a lot of the infrastructure required to deliver the service that they are doing for you.

Sagi: We hear so much about data leaks and violations related to the use of information by disgruntled employees. What is your view?

Mark: In absolute terms there are many more data leaks from companies in the U.S., the U.K. and European service companies than there are from India. Certainly it is a much more interesting story to write about data leaks from Indian companies, but I think that there is also a sense that because we are talking about people who earn a much lower wage, essentially the kind of logic goes that if we are talking about bribing insiders to bring data out of a company, then essentially it should be much cheaper to do that. That is the kind of key worry that people have when they look at a place like India. But if you wanted to do a run-down of the most data leaks, probably you would find the U.S. at the top anyway.

Mark: The immediate myth is that it is 10 times cheaper than doing work in the United States or in Western Europe — this idea that you can get greater quality/lower price. It is kind of sold as a myth that you can have it all basically. You can reduce your running costs, you can increase productivity, increase efficiency, re-engineer your processes — and at the same time, it is cheaper as well. It sounds impossible and really, to be honest, it is. It is true that operating costs are lower in an environment like India, but the whole restructuring of the way that you operate and the fact that you may need to entirely re-engineer your supply chain to fit your Indian supplier in the supply chain, or you may need to completely restructure the way you are doing business.

Sagi: Can you describe NASSCOM and its role?

Mark: NASSCOM is the National Association of Software and Service Companies, and it is a Chamber of Commerce. It is representation of the IT services industry in India. It’s got more than 1,000 member companies. They have been around since the ’80s, so they are quite well-established, and given that their membership is 95 or 96 percent of the Indian high-tech IT and service industry, they are the voice of the industry. NASSCOM has been...
instrumental in actually trying to obtain changes to the IT Act of 2000. They have tabled amendments that they would like to make to the legislation to improve the situation around intellectual property and data protection, and it is true that it is basically sitting with the government at the moment. It is something that is promised to be introduced.

Sagi: NASSCOM has been pushing for more self-regulation opportunities for its constituents. Can you describe some of the activities and some of the actions NASSCOM has been taking from a self-regulation perspective for its members?

Mark: India and the high-tech industry have exploded since the millennium, and they have embraced data protection. They have taken on this role almost like policemen of the industry. They have taken on the role of training the law enforcement officers in India, so NASSCOM is actually now working its way through training the police in India to understand cybercrime and problems around information technology. More importantly, they have set up a national skills registry — which was really a reaction to some of the data leaks that we have seen. They have tried to create this idea that people who work in the industry in India want to be trusted. So they have created a safe harbor where you can upload your résumé basically, so it is a complete history of where you have worked, who you have worked with, references you can give about the quality of your work. So if you are working within a BPO company (Business Process Outsourcing), then it becomes the de facto standard that the employer will check this National Skills Registry and have a look at your verified background before hiring you.

Sagi: If I am a Western company concerned about privacy and data protection, does it make more sense for me to offshore my operations to create a sub-company or an additional company that is mine rather than outsourcing my services to a vendor?

Mark: That question changes depending on each company and the exact details of the type of service they are trying to offshore. In general, I guess we have observed in the marketplace is that where there is a great deal of personal data or data that could be utilized in some way, whether that is personal data about plants or about the business that the company performs, quite often we have seen that offshored rather than outsourced. I am thinking the best example is within investment banking, where you are looking at quite a lot of banks that have chosen to set up their own facilities. They have their own office located in India and they hire their own staff and put those people on their own contract.

India and Outsourcing continued from page 7

Mark: I have certainly shown up at a couple of BPOs myself. There can be a difference definitely between the kind of an unannounced visit where you just walk in, and then where you are actually greeted at the gate by the head of the company. At one particular company in Chennai, I just strolled into the campus. There was a security guard who was supposed to be checking for USB keys, cameras, phones, any kind of recording device. But I gave him just one item, which was enough to keep him happy. I gave the guy my laptop computer, but I still had a phone in my pocket and a couple of USB keys. You need to make sure that there is not just a façade of security and that it is actually a reality. The only way you can really do that is just to test them out yourself.

Sagi: Have you been familiar with stories of that type of second unannounced visit that yielded other information?

Mark: I should do when selecting potential customers will be with the CEO coming down to welcome you at the gate and giving you a tour of the facilities. But I would say that definitely you should also come back unannounced. Ask to see the boss again the next day when they are not expecting you to show up. See if you can still observe all the same security procedures in place in that environment.

Sagi: OK, so I have made the decision to outsource my services to an Indian company. What kind of steps should I be taking before I am selecting a vendor to work with? What would be the type of due diligence, the type of review, that I should do when selecting potential outsourcing companies?

Mark: Make sure that you know who they are hiring and where they are coming from so that you can get verified backgrounds from the NASSCOM skills registry. If you are going out on the ground in India, you need to make at least a couple of visits to each location where you are considering possibly using them. The typical kind of visit as a potential customer will be with the CEO coming down to welcome you at the gate and giving you a tour of the facilities. But I would say that definitely you should also come back unannounced. Ask to see the boss again the next day when they are not expecting you to show up. See if you can still observe all the same security procedures in place in that environment.

Don't miss Part 2 of this Q&A next month in the Advisor. The entire interview is available for sale on the IAPP’s Web site, www.privacyassociation.org.
Privacy and data governance can be a compliance cost or a business enabler. KPMG helps our clients understand, prioritize, and control the risks associated with the use, transfer, storage, or management of critical information assets.

Our global team provides a full range of privacy advisory services with a multidisciplinary approach that uses formalized regulatory, forensic, and technology methodologies. It’s a valuable combination that can help your business.

For information, contact Doron Rotman, National Privacy Service Leader, IT Advisory at 650-404-4176, email drotman@kpmg.com.

www.us.kpmg.com
Do any laws cover the sending of marketing messages to cell phones?

In the U.S. there are some statutory and regulatory restrictions on sending promotional messages to cell phones and other wireless devices. (Much of the impetus for regulation arose from the fact that consumers have to pay to receive these messages.) The laws and rules that intersect in this space are CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act) (15 USC §§7701-7713) and the Federal Communications Commission’s (FCC) Wireless Email Rule (64 CFR §64.3100), which was promulgated pursuant to CAN-SPAM and covers “Mobile Service Commercial Messages” (MSCM), assuming that the primary purpose of the message is commercial.

Under CAN-SPAM, wireless service providers were supposed to create special domains for their customers to use for sending and receiving “mobile service messages”; and the Telemarketing and Consumer Fraud and Abuse Prevention Act (TCFAP) (15 USC §§6101-6108), the Telephone Consumer Protection Act (TCPA) (47 USC §227), and the Telemarketing Sales Rule (TSR) (16 CFR §310.1 et seq.) along with the national Do Not Call registry that the Federal Trade Commission (FTC) maintains (www.donotcall.gov). Some states also have their own Do Not Call registries, so telemarketers have to be familiar with those laws, too.

The easiest way to figure out which laws and rules apply to a promotional message is to look at the destination to which the message is being sent. If the destination is an email address — with a “@” and a domain — CAN-SPAM and the FCC’s wireless email rule apply. If the destination is a telephone number, then the TCFAP, TCPA and TSR apply.

CAN-SPAM covers traditional email messages, as well as text (also known as SMS or Short Message Service) messages, and MMS (Multi-media Messaging Service) messages that contain graphics, video and audio components. These formats all fall within the FCC’s definition of a “Mobile Service Commercial Message” (MSCM), assuming that the primary purpose of the message is commercial.

Under CAN-SPAM, wireless service providers were supposed to create special domains for their customers to use for sending and receiving “mobile service messages.” These specific domains are required to be listed on the FCC’s Wireless Domain Registry (available at www.fcc.gov/cgb/policy/DomainNameDownload.html).

If the primary purpose of a “mobile service message” is commercial, the sender needs “express prior authorization” from the recipient to send it. “Express prior authorization” can be obtained by oral or written means, including electronic methods. A sender may obtain the subscriber’s express prior authorization to transmit MSCMs to that subscriber in writing. Written authorization may be obtained in paper form or via an electronic means, such as an electronic mail message from the subscriber. It must include the subscriber’s signature and the electronic mail address to which MSCMs may be sent. Senders who choose to obtain authorization in oral format also are expected to take reasonable steps to ensure that such authorization can be verified.

Because the consent standard for sending Mobile Service Commercial Messages is so high, the usual practice is for commercial emailers and Email Service Providers (ESPs) to block all emails going to the domains listed on the FCC’s Wireless Domain Registry.

But, in its “Primary Purpose” Rule (16 CFR §316.3), the FTC recognized that emails can contain mixed content, i.e., both commercial content and content that is not commercial. If an analysis of a message intended to be sent to an email address that contains a domain listed on the FCC’s Wireless Domain Registry concludes that the primary purpose of a mixed content message is NOT commercial, then the sender doesn’t need the recipient’s express consent to send it. It should be noted that the “express consent” requirement does not pertain to forwarded messages, unless there’s an inducement or consideration offered for forwarding the message.

The TCPA and TSR also cover telemarketing SMS (text) as well as voice messages.

The TCPA was enacted in 1991 to address certain telemarketing practices, including calls to wireless telephone numbers, which Congress found to be an invasion of consumer
privacy and even a risk to public safety. The TCPA specifically prohibits calls using an automatic telephone dialing system or artificial or prerecorded message “to any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service, or other common carrier service, or any service for which the called party is charged.” (47 USC §227[b][1][A][iii]). The TCPA defines an “automatic telephone dialing system” as “equipment which has the capacity (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers.” (47 USC §227[a][1]) The CAN-SPAM Act provides that “nothing in this Act shall be interpreted to preclude or override the applicability” of the TCPA. (15 USC §7712[a]).

In 2003, the FCC released a Report and Order in which it reaffirmed that the TCPA prohibits any call using an automatic telephone dialing system or an artificial or prerecorded message to any wireless telephone number. This includes both voice calls and SMS text messaging calls to wireless phone numbers.

The Telemarketing and Consumer Fraud and Abuse Prevention Act (TCFAP) gave the FTC the authority to promulgate the Telemarketing Sales Rule (TSR) (16 CFR §310.1 et seq.). The TSR prohibits telemarketers from engaging in various deceptive acts or practices, and imposes recordkeeping requirements. One section of the TSR created the National Do Not Call Registry (16 CFR §310.4[b][1][ii][B]). If a wireless telephone number is listed on the National Do Not Call Registry, a marketer is prohibited from calling that number unless it has an “established business relationship” with the consumer. An “established business relationship” is defined as “a relationship between a seller and a consumer based on (1) The consumer’s purchase, rental, or lease of the seller’s goods or services or a financial transaction between the consumer and seller; or (2) The consumer’s inquiry or application regarding a product or service offered by the seller, within the eighteen (18) months immediately preceding the date of a telemarketing call; or (3) The consumer’s inquiry or application regarding a product or service offered by the seller, within the three months immediately preceding the date of a telemarketing call.” (16 CFR §310.2[n]).

As marketers seek to utilize new technologies to promote their products, they need to become familiar with existing laws under which their activities may fall, as well as to keep abreast of new legislation that may affect the ways they interact with their existing and prospective customers.

Elise Berkower, an attorney and CIPP, is the Executive Vice President of Privacy Strategy at Chapell & Associates, a leading strategic consulting firm focusing on privacy, marketing and public policy. Prior to joining Chapell & Associates, she served as DoubleClick’s Senior Privacy Compliance Officer for six years, helping DoubleClick’s ad serving, search, Web site analytics, email and direct marketing clients address privacy issues. She participates in many privacy and technology industry groups, and is a member of the Advisory Board of The Privacy Advisor. She can be reached at elise@chapellassociates.com.

This response represents the personal opinion of our expert (and not that of his/her employer), and cannot be considered to be legal advice. If you need legal advice on the issues raised by this question, we recommend that you seek legal guidance from an attorney familiar with these laws.
The Privacy Advisor (TPA): What are your responsibilities in the UK?

Thomas: As Information Commissioner my role is to promote people’s access to official information and protect people’s privacy. On the privacy side my Office enforces the Data Protection Act and the Privacy and Electronic Communication Regulations. These implement for the United Kingdom two European Union Directives which provide a broadly harmonized approach across all 27 EU countries. The Data Protection Act safeguards the handling of personal information and provides important rights. In most situations, individuals can find out what information the state and other organizations hold about them and get it corrected if that information is wrong. Some 22,000 people contact my Office each year because they feel their privacy and other rights may have been infringed.

My Office also enforces the UK Freedom of Information Act. This is relatively new legislation, but we have already played a major role in ensuring more and more official information is in the public domain, from farm subsidies to travel expenses for Members of Parliament.

TPA: Your Office recently published a well-publicized report on a Surveillance Society. Can you describe the report?

Thomas: In November I was delighted to host the 28th International Data Protection and Privacy Commissioners’ Conference in London. I called for a public debate on the implications of living in a surveillance society and I gave a serious warning that we are waking up to a surveillance society. The theme struck a chord within the UK and worldwide. To coincide with the conference, we published ‘A Surveillance Society’ — a detailed report on surveillance now and projections for what our society might be like in 2016. It describes a surveillance society as one where technology is extensively and routinely used to track and record our activities and movements. This includes systematic tracking and recording of travel and use of public services, automated use of CCTV, analysis of buying habits and financial transactions, and the workplace monitoring of telephone calls, email and Internet use. This can often be in ways which are invisible or not obvious to ordinary individuals as they are watched and monitored, and the report shows how pervasive surveillance looks set to accelerate in the years to come.

As ever-more information is collected, shared and used, it intrudes into our private space and leads to decisions which directly influence people’s lives. Mistakes can also easily be made with serious consequences — false matches and other cases of mistaken identity, inaccurate facts or inferences, suspicions taken as reality, and breaches of security.

At the conference, Data Protection and Privacy Commissioners from around the world agreed on a communiqué that set out how we will ensure privacy is effectively protected in the surveillance society. My Office will shortly publish a follow-up report to identify the next steps we will take as a regulator in this important area.

TPA: One of your priorities has centered on ‘pre-texting’ or ‘blagging.’ Can you tell us more?

Thomas: Yes — in the UK we use the term blagging. Personal information is usually obtained by making payments to staff or impersonating the target individual or another official. Some victims are in the public eye; others are entirely private citizens.

Last year, I urged the UK Government to amend the Data Protection Act and introduce a jail term for those convicted of obtaining and selling personal information. We uncovered an existence of a widespread industry devoted to illegally buying and selling people’s personal information. I issued a special report to the UK Parliament, ‘What Price Privacy?’ which explained how some individuals trade people’s personal information, such as current addresses, details of car ownership, ex-directory telephone numbers or records of calls made, criminal records and bank account details. Private investigators, tracing agents and their operatives — often working loosely through several intermediaries — are the main suppliers.

The ultimate buyers of illegally obtained personal information include journalists, financial institutions and local...
authorities wishing to trace debtors; estranged spouses seeking details of their ex-partner’s whereabouts or finances; and criminals intent on fraud or witness or juror intimidation.

The report arises from investigations carried out by my Office, sometimes using search warrant powers. Documents seized during one raid revealed evidence of a large scale market in the trading of personal information. However, the existing penalties are low and do not have a deterrent effect. One major case resulted in conditional discharges for the perpetrators.

To highlight the extent of this illegal trade, I also recently published a league table of media publications showing which are the most prolific buyers of unlawfully obtained personal information. The list is based on evidence found in just a single raid that my Office carried out at the premises of a private investigator.

Recently the government confirmed that it will amend the UK Data Protection Act. I am delighted the Government has now decided to adopt my proposals to introduce tougher penalties to deter people from engaging in the deliberate misuse of personal information.

TPA: What are you doing to help the British people look after their personal information?

Thomas: New figures we released in January revealed Britons are leaving themselves vulnerable to identity theft by not taking enough care to protect their personal information. In fact, a fifth believe they have been a victim of identity crime. We conducted a nationwide survey uncovering how easy Britons make it for criminals to steal their identity. A third of those surveyed admitted to throwing away personal documents such as bank statements and receipts without shredding or destroying them, a quarter of people do not routinely check bank statements for unfamiliar transactions and almost half of those surveyed use the same PIN and password across different accounts.

The research was published to coincide with the launch of a personal information toolkit, aimed at helping individuals protect their personal information more easily. We are encouraging people to use the personal information toolkit which provides individuals with advice and tips on protecting their information.

“Britons are leaving themselves vulnerable to identity theft by not taking enough care to protect their personal information. In fact, a fifth believe they have been a victim of identity crime.”

TPA: And what is the UK government doing?

Thomas: Privacy issues are now high on the news agenda in the UK. I used my annual report last year to highlight that data protection provides a valuable framework for sharing personal information across the public sector, and should not be seen as a barrier. This issue is now central to many high profile UK government initiatives, such as identity management, health and education.

There are clear benefits to sharing more information — safeguarding the public, improving services and reducing costs. However, I have stressed that government and other public bodies must retain public trust and confidence, and will only achieve this if they share personal information in a secure, lawful and responsible way. I do not want data protection to be wrongly blamed for preventing sensible information sharing, for example to detect crime, protect children at risk or prevent fraud. Electronic government initiatives which improve public services, such as online car tax renewal, show that information can be shared in entirely acceptable ways.

But as more and more information is passed from one database to another, it is important to get the basics right. Trust and confidence will be lost if information is inaccurate or out of date, if there are mistakes of identification, if information is not kept securely or if reasonable expectations of privacy are not met. There must be clarity of purpose — not just sharing because technology allows it. And people must be told how their information is being shared and given choices wherever possible.

Data protection should be seen as part of the solution, not as the problem. The eight core principles that underpin the Data Protection Act provide a widely supported framework to make sure personal information is collected in ways which are necessary, justified and proportionate. Getting it right — at both design and operational levels — is vital to ensure the public trust and confidence which is needed to deliver the benefits of information sharing.

My Office intends to contribute constructively to government thinking and feed in data protection expertise. It is our job to promote good practice and we will be exploring ways — for example through information-sharing guidelines and promoting statutory codes of practice — to bring greater certainty and clarity to help government achieve the right balance.

TPA: And what about Freedom of Information — is it working?

Thomas: Since I have been Commissioner, we have seen the introduction of the Freedom of Information Act. The
Harriet Pearson, IBM’s CPO, Testifies in Support of Bill Banning Genetic Testing Discrimination

Harriet Pearson, CIPP, VP of Corporate Affairs & Chief Privacy Officer, IBM Corporation, and an IAPP board member, recently testified before a House subcommittee during a hearing on “Protecting Workers from Genetic Discrimination.”

In October 2005, under Pearson’s guidance, IBM became the first major corporation to add genetics to its discrimination policy, prohibiting “current or prospective employees’ genetic information from being used in any employment decisions.” IBM supports federal legislation preventing discrimination based on genetic information. The bill, which has passed the Senate twice in the past, was reintroduced in the House in January with bipartisan support. If passed, it would give genetic information the same confidentiality as medical records, and make it illegal for employers and insurance companies to use individuals’ genetic information when make hiring or coverage decisions.

Pearson’s testimony generated media coverage, including a CNET News piece.

Current and Former IAPP Board Members Appointed to TRUSTe Board of Directors

TRUSTe, an online privacy certification organization, recently appointed Jules Polonetsky, CIPP, Chief Privacy Officer and Senior Vice President of Consumer Advocacy at AOL, and former IAPP board member, to its board of directors. Polonetsky joins other IAPP board members on the TRUSTe board, Peter Cullen, CIPP, Chief Privacy Strategist at Microsoft Corporation, and David Hoffman, CIPP, Group Counsel and Director of Privacy at Intel Corp. Hoffman is Assistant Treasurer of the IAPP Board.

TRUSTe’s board of directors consists of 11 members selected for their strong backgrounds in a variety of industries relating to online privacy, trust and business. The board oversees the nonprofit’s long-term strategy and programs.

Appointed along with Polonetsky to the TRUSTe board were two other new members: Jonathan Hart, a member in the Media and Information Technologies group at the law firm Dow Lohnes PLLC, and Donald Whiteside, Vice President of the Corporate Technology Group and Director of Technical Policy & Standards at Intel. TRUSTe is an independent, nonprofit organization that identifies trustworthy online organizations through its Web Privacy Seal, Email Privacy Seal and Trusted Download Programs certifications.
Background: The Standing Committee on Access to Information, Privacy and Ethics is currently conducting interviews in preparation for a report to Parliament on changes to Canada’s Personal Information Protection and Electronics Document Act (PIPEDA). Nymity, on behalf of The Privacy Advisor, recently interviewed Tom Wappel, MP, Scarborough Southwest, who also serves as Chairman of the Standing Committee on Access to Information, Privacy and Ethics.

The Privacy Advisor (TPA): How does the regulatory review of PIPEDA process work? What are the goals?

Wappel: The act mandated that a Parliamentary Committee review the operation and effectiveness of the act, five years after it came into force. This review was referred to our committee by the House of Commons. Our committee decided to hear from interested stakeholders, the public, the Minister of Industry and, of course, the Privacy Commissioner. The goals are to try to identify if there are any shortcomings in the act, based on the experience since it came into force, and make recommendations to the Minister on how to improve the act.

TPA: Who is on the committee?

Wappel: The Committee is composed of 12 Members of Parliament: 5 Conservatives, 4 Liberals, 2 Bloc Quebecois and 1 NDP member. As you can see, the opposition members outnumber the government members. This is reflective of a minority Parliament.

TPA: Who is presenting to the committee and how were they selected?

Wappel: The committee, through its Steering Committee, in consultation with the Clerk of the Committee and the committee’s research staff, decided on a list of witnesses, representative of the various groups. An invitation also was broadcast for interested parties to indicate to the clerk their interest in either appearing before the committee or submitting a written brief. Respondents also were considered by the steering committee. The goal was to have a broad and diverse group of interveners.

TPA: What have been the key areas of concern by presenters so far?

Wappel: Some presenters have felt that the act is more or less fine the way it is. Others have suggested that the Privacy Commissioner have order-making powers; that there be a definition of “work product” contained in the act; that there be some sort of mandatory security breach notification mechanism; that there be the ability to more readily exchange information if it is in furtherance of potential fraud or other criminality; that it be easier for potential purchasers to obtain relevant information from sellers prior to purchase of the business; and that there be some recognition of the speed of development of the information highway; the potential exploitation of children on the Internet; and the international aspects of the Information Age. That is just a short synopsis of some of what we have heard so far.

TPA: What are the key areas of concern for the committee?

Wappel: The key concern of the committee is to ensure that all those who wish exchange information if it is in furtherance of potential fraud or other criminality; that it be easier for potential purchasers to obtain relevant information from sellers prior to purchase of the business; and that there be some recognition of the speed of development of the information highway; the potential exploitation of children on the Internet; and the international aspects of the Information Age. That is just a short synopsis of some of what we have heard so far.

See, PIPEDA Review, page 16
to present either do so, submit a brief or have their concerns aired by others. We want to try to make sure that the act will operate in the fairest and most efficient way possible into the future.

TPA: What happens after the review is complete? What are the steps to amend PIPEDA?

Wappel: Upon the completion of the hearing of evidence, the committee will draft a report to the government. We hope it will be unanimous, but it may not be. There may be concurring reports with additional comments, or there may be dissenting reports, however, there will certainly be a majority report. Once the report is finalized and passed by the committee, it is presented to the House of Commons, for the attention of the government. The usual practice is for the relevant ministry to consider the report and draft a response for approval by its minister, who will then have Cabinet approve the final response, which will be tabled in the House of Commons. This may take up to 180 days approximately. The response usually contains a detailed list of the recommendations of the committee which the government will accept, or reject, with the reasons why.

TPA: What happens if an election is called?

Wappel: If an election is called before the committee issues its report, the work of the committee is effectively lost. A new Parliament will decide how it wants to deal with the fact that a report on PIPEDA has not been submitted to Parliament, despite the clear wording of the act. Usually, but not always, the new committee would adopt the previous committee’s report, resubmit it to the new House and request a response from the new government. However, there is nothing this committee can do to bind a future committee to a particular course of action. If an election is called after the government issues its response, but before any recommendations are implemented, the newly elected government is not bound to follow the response of the previous government.

TPA: When would we expect PIPEDA to be amended?

Wappel: It is only a guessing game as to when amendments to PIPEDA would be forthcoming. I would expect that, before any major recommendation were implemented, the ministry would hold consultations with stakeholders to discuss how most efficiently to implement the changes.

TPA: In what form would PIPEDA be modified? Could the Canadian Standards Association principles be modified?

Wappel: It is too early to comment on the form of modifications to PIPEDA, if any, as we are still hearing evidence and have not yet begun to discuss our draft report.

TPA: Have there been any concerns relating to Quebec’s constitutional challenge of PIPEDA?

Wappel: The issue of Quebec’s constitutional challenge to PIPEDA has been raised by some witnesses and committee members. As far as we can tell, the matter is stalled in the courts. Until the courts advise otherwise, we have to assume that the act is constitutional.

TPA: In closing, what else is on the agenda for the committee?

Wappel: The committee’s first report of this Parliament called upon the Minister of Justice to prepare and submit to Parliament a new Access to Information Act, by December 15, 2006, for consideration by the committee. This did not happen. The committee has requested the Minister of Justice to appear before the committee this month, to discuss this issue further. The committee is also aware that the Privacy Act is in need of review and modernization.

Party: Liberal


Chairman, Standing Committee on Access to Information, Privacy and Ethics, Past Chairman of the Standing Committee on Fisheries and Oceans, Member, Subcommittee on the Review of the Anti-Terrorism Act of the Standing Committee on Public Safety and National Security, Past Member and Past Chairman of the Subcommittee on National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness, Member, Past Chairman and Past Vice-Chairman of the Joint House of Commons and Senate Standing Committee on the Scrutiny of Regulations, Co-Chairman of the Canada-China Legislative Association and Chairman of the Canada-Hungary Parliamentary Friendship Group. Past Member of the Standing Committee on Citizenship and Immigration.

Education: University of Toronto, 1971 (B. Arts) (Pol. Sci.); Queen’s University, 1974 (L.L.B.); Called to the Bar of Ontario, April 8, 1976

Nymity (www.nymity.com) provides Web-based privacy management support solutions that help organizations manage the risks that lead to a data breach, a privacy complaint and to non-compliance or over-compliance with privacy laws.
Congratulations, Certified Professionals!

The following individuals successfully passed the CIPP, CIPP/G and/or the CIPP/C exam. Please join the IAPP in saluting these graduates!
Results of a survey sponsored by EpicTide, a provider of security solutions for the healthcare industry, yielded some interesting findings about consumer awareness of medical identity theft and patient safety concerns.

The survey questions were designed to elicit information from consumers about the rate of medical identity theft; understanding of their patient rights; and perceptions regarding the ability of healthcare organizations to protect patient records, ensure patient safety and report security breaches.

One of the key findings, according to the survey, is that nearly half of the survey participants had never heard of medical identity theft — despite the increase in medical ID theft and recent media coverage. Consumers also are mostly unaware of the consequences associated with medical identity theft, the survey found. Although respondents were somewhat able to identify examples of medical ID theft, the survey concludes that additional consumer education is needed.

Another critical finding of the survey is that there is a great deal of confusion among participants as to their privacy rights. Although all doctors’ offices, pharmacies and medical organizations require patients to sign a HIPAA notice, only 53 percent of survey respondents reported being asked to sign a notice of their HIPAA rights at a doctor’s office, hospital, pharmacy or other medical organization. Additionally, half of the participants responded that they did not read the HIPAA notices that they have been asked to sign.

The survey goes on to reveal that the greatest misperception reported in regard to patient rights is that participants believed that “employees of healthcare organizations may legally access or view their records without written consent for reasons other than providing care or medical goods, or for billing/payment purposes.”

The survey also asked participants a series of questions regarding the responsibility of healthcare organizations in reporting security breaches. While just more than 98 percent responded that healthcare providers should be accountable for informing patients if they suspect patient records have been accessed or compromised without authorization, 70.8 percent do not believe that healthcare providers are diligent about informing patients of suspected security breaches.

More information on accessing the survey is available at www.epictide.com.

---

**Consumer responses to a survey asking whether they believe their healthcare providers know when someone accesses their medical records**

- One in two consumers believe their healthcare provider does not know when someone accesses their medical records.
- 39.9 percent of consumers feel confident that their healthcare providers are able to secure their medical records and personal information.
- 50.1 percent feel their healthcare providers are effective in protecting their medical records.

*Source: EpicTide*

**Consumer Beliefs Regarding the Consequences of Identity Theft**

- 92.7 percent of respondents associate receiving bills for medical care that they did not receive as a possible consequence of medical identity theft.
- 83.5 percent of respondents associate increased cost of medical insurance as a possible consequence of medical identity theft.
- 82 percent of respondents associate increased cost of overall medical care as a possible consequence of medical identity theft.
- Only 75 percent of respondents associate altered medical records such as allergies or blood type or severe medical errors, complications or death as possible consequences of medical identity theft.
- 70.8 percent of respondents agree that medical identity theft is a cause of rising healthcare costs.

*Source: EpicTide*
A Day in the Life of an Entrepreneur: Nymity’s Terry McQuay

The Toronto Star recently caught up with Terry McQuay, CIPP, CIPP/C, founder of Nymity, a startup information technology company providing online risk management solutions related to privacy issues and regulatory compliance.

After being tapped by The Star as a finalist in its “2007 Build a Business Challenge,” Nymity was approached by venture capital firm, Ventures West, which saw an opportunity in Nymity, especially given the growth of privacy legislation and a newly implemented Canadian law requiring companies to have a privacy officer. The Star profiled McQuay as he sat down with Robin Axon of Ventures West and explained the origin of Nymity and its growth. The article follows McQuay through a bevvy of meetings on topics ranging from revamping Nymity’s Web site, to analyzing its pricing strategy to identifying a spokesperson for the business. The full article is available at www.nymity.com/about_us/TheStar.asp.

Cavoukian Calls for Privacy Legislation in Ontario

Ontario Information and Privacy Commissioner Ann Cavoukian again pushed for privacy legislation in the province in reaction to comments from Government Services Minister Gerry Phillips. Phillips has called upon the Canadian government to force banks and retailers to notify customers about privacy breaches, but Cavoukian is in favor of provincial legislation addressing breach notification and other privacy issues.

Ontario is the only one of Canada’s four largest provinces that does not currently have private-sector privacy legislation. B.C., Alberta and Quebec currently have legislation in place.

In a news release issued by her office, Cavoukian stated, “Instead of pointing to Ottawa, Ontario should be taking responsibility for bringing in its own legislation (like the three provinces cited), that will address Ontario’s privacy needs, including a key provision to require breach notification.”

Americans Vote USPS #1 for Privacy

The United States Postal Service was rated the number one agency Americans trust to protect their privacy, according to the “2007 Privacy Trust Study of the United States Government” conducted by The Ponemon Institute LLC. This is the third year in a row that the USPS held the top spot, attaining a privacy trust score of 83 percent. Results also showed that the USPS increased customer satisfaction and trust scores from last year.

The study, which surveyed more than 7000 people, identified 10 key factors — from a sense of security when providing personal information to Web site security to access to personal information — when ranking 60 federal agencies. The purpose of the study is to gauge Americans’ confidence level in the government agencies that routinely collect and use citizens’ personal information.

VeriChip Completes IPO

VeriChip, which develops, markets and sells radio frequency identification, or RFID, systems used to identify, locate and protect people and assets, recently announced the pricing of its initial public offering.

The company is offering 3,100,000 shares of its common stock at $6.50 per share, before underwriting discounts and commissions. VeriChip’s common stock will be traded on the NASDAQ Global Market under the symbol “CHIP”, according to a company news release.

Merriman Curhan Ford & Co. is the book-running manager for the offering and C.E. Unterberg, Towbin and Kaufman Bros., L.P are co-managers.

In addition to the shares being offered by VeriChip, Applied Digital Solutions, Inc., the company’s largest shareholder, has granted the underwriters a 30-day option to purchase up to an additional 465,000 shares of the company’s common stock to cover over-allotments, if any.

The offering of these securities is made only by means of a prospectus, copies of which may be obtained from Merriman Curhan Ford & Co., 600 California St., San Francisco, Calif., 94108 (telephone 415-248-5600 or fax: 415-248-5690).
public has a right to know what is done in their name with their taxes. This is a hugely important piece of legislation and is opening up more and more information to public scrutiny.

My Office has published some powerful rulings on a wide range of issues including the cost of identity cards, Legionnaires disease, academic standards and salaries of senior officials. It is extremely encouraging to see the positive impact the Freedom of Information act is having on individuals. A great deal of information has been released since the introduction of the act, which would not otherwise have been in the public domain. I was delighted that Parliament's Constitutional Affairs Select Committee concluded that freedom of information was proving to be a significant success.

Since the Act came into force, the ICO has received some 5,000 complaints and closed around three quarters of these cases.

TPA: What are some of the privacy issues on the horizon from your perspective?

Thomas: There is no doubt that privacy issues continue to rise fast up the agenda — politically and commercially — in the United States and worldwide. People want their privacy and personal information properly respected. Businesses and governments want to get it right. Computing power gets ever-stronger. There can be very difficult balances to draw, especially where there may be tensions with the battles against terrorism and serious crime.

My Office's overall approach is to take a practical and down-to-earth approach — simplifying and making it easier for the majority of organizations that seek to handle personal information well, but tougher for the minority who do not.

One of the major hot topics is the current lack of synergy between privacy laws around the world. As pressures build for a clearer legal framework within the U.S., I want to remind everyone of the benefits of maximum global harmonization. Equally, I recognize that the EU Data Protection Directive is widely seen as excessively bureaucratic and prescriptive, not always concentrating on the priority real risks to individuals. There are current initiatives in Europe to make data protection more effective and better communicated in practice. We may not yet meet in the middle, but how much scope is there to move closer?