Centre for Information Policy Leadership
Hunton Andrews Kurth

21 August 2019

**Comments by the Centre for Information Policy Leadership on Justice Canada's Technical Engagement with Experts on the Modernization of Canada's Federal Privacy Act**

On 18 June 2019, the Canadian Department of Justice, Public Law and Legislative Services Sector reached out to the Centre for Information Policy Leadership (CIPL),[1] along with a group of other experts, to seek input on various discussion papers it has produced that are relevant to its review[2] of Canada's federal public sector privacy law, known as the Privacy Act.[3]

CIPL welcomes the opportunity to participate in this technical engagement and commends Justice Canada for thinking so carefully and deeply about the issues it sets forth in the discussion papers. CIPL's response will focus mainly on two of the five consultation papers, namely, the second paper on "Transparency and accountability: demonstrating the commitment and respect necessary to facilitate trust"[4] and the fourth paper on "A modern and effective compliance framework with enhanced enforcement mechanisms".[5]

Through its comments below, CIPL wishes to:

(1) Highlight the importance of accountability in the modern digital economy and demonstrate why it is critical that such a concept be included in any reformed version of the Privacy Act;

(2) Support the inclusion of a breach notification requirement in the Privacy Act and elaborate on the standard that such a requirement should reflect, taking into account the experience of the private sector; and

(3) Underline the important role privacy regulators play with respect to oversight of public sector organizations and explain how a revised version of the Privacy Act can facilitate regulators in both prioritizing and meeting their regulatory objectives and in effectively ensuring compliance by government institutions.

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 77 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.
[2] Modernizing Canada's Privacy Act, Department of Justice Canada, available at https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html.
[3] Privacy Act, R.S.C., 1985, c. P-21, available at https://laws-lois.justice.gc.ca/eng/acts/P-21/.
[4] Privacy Act Modernization: A Discussion Paper – 2. Transparency and accountability: demonstrating the commitment and respect necessary to facilitate trust, Department of Justice Canada (non-public discussion paper).
[5] Privacy Act Modernization: A Discussion Paper – 4. A modern and effective compliance framework with enhanced enforcement mechanisms, Department of Justice Canada (non-public discussion paper).

## I. CIPL Comments on Privacy Act Modernization: A Discussion Paper – 2. Transparency and accountability: demonstrating the commitment and respect necessary to facilitate trust

### Accountability

CIPL fully agrees with the explanation and discussion of accountability in Discussion Paper 2. What follows are our answers to some of the specific questions posed in the paper on the topic of accountability.

**Q.2(a): Should a privacy management program be formally required of government institutions under the Privacy Act or should institutions be given greater flexibility to independently structure their own compliance efforts?**

Yes, an amended Privacy Act should include a requirement that all government institutions that collect, handle, use and otherwise possess personal information implement a privacy management program. As Discussion Paper 2 notes, accountability requires "accountability measures" – i.e. "internal capacity, tools and processes" that operationalize and enable compliance with privacy responsibilities and requirements. Such capacity, tools and processes are best provided for through formal and comprehensive privacy management programs. CIPL is in full agreement with the paper's characterization of such programs and the benefits they bring.

For many years now, CIPL has promoted the concept of organizational accountability as a key building block of effective privacy and data protection and has urged giving effect to accountability in privacy laws through comprehensive organizational privacy management programs that cover all core elements of organizational accountability (see discussion of core elements below). We have discussed organizational accountability and its role in global data protection in detail in a number of white papers,[6] and have held many workshops and other events on this topic with multi-stakeholder participants including global data protection authorities (DPAs) and law and policy makers. Advocating for organizational accountability is at the core of CIPL's mission and one of our most important current work streams.

Comprehensive privacy management programs that are designed to operationalize relevant privacy requirements, promote compliance and ultimately engender increased digital responsibility as well as trust among data subjects are equally relevant to the public and private sectors. All effective privacy protections, whether in the public or private sectors, start with, and flow from, having the right processes, tools and procedures in place that enable such protections. Privacy programs that cover the whole range of core elements of accountability can deliver and, indeed, are necessary for delivering, the appropriate

[6] See CIPL white papers on "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society", 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability", 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf; and CIPL Accountability Q&A, 3 July 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_q_a__3_july_2019_.pdf.

compliance and trust outcomes in both the public and private sectors. Accordingly, all government departments should have such privacy programs, tailored to their specific needs.

Indeed, one of the key features of the accountability-based privacy management approach is that it is scalable, flexible and adaptable to the specific organization and the data processing context at hand. For example, because risk assessment is a core element of any accountability-based privacy management program, organizations will be in a position to base the features of their particular privacy programs and their relevant privacy protections and controls on the specific privacy risks to individuals posed by their processing activities. Thus, this approach is not a one-size-fits all approach but allows for variation between organizations as to how to deliver privacy through a privacy program that is tailored to their needs. Thus, we do not see a contradiction between requiring all government organizations to have comprehensive privacy management programs and also allowing them the necessary flexibility to independently structure their compliance efforts within a general accountability-based privacy management framework required by the Privacy Act. Not only would such privacy management programs enable the effective implementation of, and compliance with, applicable privacy protections, having such formal programs would also enable the ongoing monitoring for effectiveness and improvement of such programs, as well as facilitate demonstrating the existence and effectiveness of these programs on request by relevant parties, including the Privacy Commissioner in an enforcement context.

**Q.2(c): What core issues should be required to be addressed in a privacy management program?**

A privacy management program should address all issues relevant to the proper governance of the entire data life cycle, from collection, use, storing, sharing and disposal. The core elements of accountability are: leadership and oversight; risk assessment; policies and procedures; transparency; training and awareness; monitoring and verification; and response and enforcement.


*Fig. 1 – The Core Elements of an Accountability-based Privacy Management Program*

Many privacy laws map to these core elements of accountability and address these elements in some fashion. A privacy management program based on these core elements may be designed to implement the substantive requirements of a specific law and may also include additional measures that are not specifically listed in the law but that spell out in greater detail general principles set forth in the law or implement one or more of the core elements of accountability. For example, a law might include a general requirement of relevant and understandable transparency or disclosures and the privacy management program might set forth more granular and specific transparency measures as appropriate in the context of the organization's processing activities.

In the context of private sector compliance programs, we have elaborated on the specific tasks under each of the seven core elements as follows:

- **Establishing leadership and oversight for data protection and the responsible use of data**, including governance, reporting, buy-in from all levels of management and appointing appropriate personnel to oversee the organization's accountability program and report to management and the board.

- **Assessing and mitigating the risks** that data collection and processing may raise to individuals, including weighing the risk of the information use against its benefits. Risk assessment also means conducting periodic reviews of the organization's overall privacy program and information uses in light of changes in business models, law, technology and other factors and adapting the program to changing levels of risk.

- **Establishing internal written policies and procedures** that operationalize legal requirements, create concrete processes and controls to be followed by the organization, and reflect applicable law, regulations, industry standards as well as the organization's values and goals.

- **Providing transparency to all stakeholders internally and externally** about the organization's data privacy program, procedures and protections, the rights of individuals in relation to their data and the benefits and/or potential risks of data processing. This may also include communicating with relevant data privacy authorities, business partners and third parties about the organization's privacy program.

- **Providing training for employees** to ensure awareness of the internal privacy program, its objectives and requirements, and implementation of its requirements in line with the employees' roles and job responsibilities. This ensures that data privacy is embedded in the culture of the organization so that it becomes a shared responsibility.

- **Monitoring and verifying the implementation and effectiveness of the program and internal compliance** with the overall privacy program, policies, procedures and controls through regular internal or external audits and redress plans**.**

- **Implementing response and enforcement procedures** to address inquiries, complaints, data protection breaches and internal non-compliance, and to enforce against acts of non-compliance.

Clearly, these tasks are relevant, and their characterization adaptable, to the public sector. A privacy management program of a government body should have policies and procedures in place that correspond to each of these core elements of accountability.

**Data Breach Notification**

**Q.2(k): What should the standard be before reporting a privacy breach? For example, how should a "material" breach be defined in the federal public sector?**

CIPL supports a data breach reporting and notification requirement for government bodies. Such a requirement should mirror the new private sector breach notification requirements and employ the same harm threshold.

Responding to the above specific question, we note that Discussion Paper 2 seeks input on how a "material breach" should be defined, presumably because the Standing Committee on Access to Information, Privacy and Ethics (ETHI Committee) recommended the creation of a notification requirement for "material" breaches.

We do not believe that the standard or harm threshold for reportable or notifiable breaches in the public sector should be "material breaches". PIPEDA does not use the term "material" breach. For the sake of consistency, we believe that the harm threshold applicable to the public sector for reporting a privacy breach should be the same as the threshold that applies to the private sector – government bodies that have experienced a data breach should be required to report to the Privacy Commissioner of Canada any breaches involving personal information if it is "reasonable in the circumstances to believe" that the breach creates "a real risk of significant harm to an individual".

PIPEDA defines "significant harm" to include "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property". In addition, the relevant factors under PIPEDA to determine whether a breach creates a "real risk of significant harm" are (1) the sensitivity of the personal information; (2) the probability that the information will be misused; and (3) any other prescribed factor. CIPL believes that this standard is appropriate for both the private and public sector, however, we think it should be further clarified. Thus, we suggest that this standard should require consideration not only of the sensitivity and probability of misuse, but also its confidentiality and the volume of the data that has been breached to determine whether notice is required. As to confidentiality, for example, unauthorized access to information that is already publicly available, or was already known by the recipient, usually does not result in a level of risk requiring notification.[7] We also believe that any federal breach reporting standard for government bodies should follow as much as possible relevant guidance on data breaches from the OPC.[8]

**Q.2(l): In what circumstances should individuals be notified of breaches?**

Government bodies and the private sector should apply the same standard for notifying individuals of data breaches as the private sector. Under PIPEDA, private sector organizations must notify a breach to individuals if it is "reasonable in the circumstances to believe" that the breach creates "a real risk of

[7] See US Chamber of Commerce and Hunton Andrews Kurth, LLP, "Seeking Solutions: Aligning Data Breach Notification Rules Across Borders", available at https://www.huntonak.com/en/insights/seeking-solutions-aligning-data-breach-notification-rules-across-borders.html at page 22.

[8] "What you need to know about mandatory reporting breaches of security standards", Office of the Privacy Commissioner of Canada, available at https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/.

significant harm to the individual", (which is also the standard for reporting a breach to the OPC discussed above).

**Q.2(m): How should the question of timelines for breach notification be managed? Is a prescriptive or context-sensitive approach better?**

Under PIPEDA, a breach must be reported to the OPC "as soon as feasible after the organization determines that the breach has occurred". The same timing requirement applies to notification to individuals. Thus, PIPEDA does not impose a specific timing requirement (such as "immediately" or a specific number of days, as some jurisdictions do). Instead, it allows for flexibility in timing based on the "feasibility" of a report or notification, and an actual "determination" that a breach has occurred. CIPL agrees with that standard and recommends that the same flexible standard be applied to the public sector.

When it comes to the timing of notification of individuals, it is important to "balance the risk associated with inappropriate delays against rushed notifications".[9] Delayed notices may increase any risk of harm by not providing timely information for individuals to protect themselves. Premature and rushed notices may give organizations insufficient time to understand the nature and scope of the breach, may cause unnecessary alarm, result in consumers undertaking burdensome and unnecessary protective steps, and expose additional information to risk of compromise if the notice is made before data security is restored.[10] The standard set forth in PIPEDA gives organizations sufficient time to determine with reasonable or sufficient certainty that a breach has occurred. It also permits them to select the precise timing of the notification based on other relevant factors, such as whether notification would undermine a criminal investigation, pose a risk to national security or other issues, the presence of which would render the notification unfeasible.

As to the timing of reporting a breach to the OPC, it is important that the timing be no later than the notification to individuals because the regulator may be required to provide guidance and information to affected individuals and address relevant compliance issues by the reporting organization, whether it is public or private. By employing the same standard for notification of individuals and reporting to the OPC, PIPEDA ensures that both the OPC and individuals receive the required report or notifications at the same time. We would support employing that same approach for the public sector.

## II. CIPL Comments on Privacy Act Modernization Discussion Paper 4 – A modern and effective compliance framework with enhanced enforcement mechanisms

### Effective Regulation

CIPL fully agrees with the premise that in order for privacy rights to be effective, they must be backed up by strong legal recourse and remedies. CIPL welcomes the reference to its 2017 white paper on "Regulating for Results: Strategies and Priorities for Leadership and Engagement" (Regulating for Results)[11] in Discussion Paper 4 and believes that the results-based approach to data protection, discussed in that white paper provides the foundations for effective regulation.

[9] *Supra* note 7 at page 24.
[10] *Id.*
[11] See CIPL White Paper on "Regulating for Results – Strategies and Priorities for Leadership and Engagement", 10 October 2017, available at

**Q.4(a): Should the Privacy Commissioner have an explicit mandate for education and outreach in relation to the public sector and if so, what should it include?**

CIPL supports the Privacy Commissioner's call for express authority under the Privacy Act to conduct research and studies on issues of public importance and to engage in public education and awareness activities. Education and outreach efforts form a key component of the leadership function of DPAs and such functions should be given top strategic priority in the modern digital economy and regulatory landscape. As CIPL has previously noted in its paper on Regulating for Results, it is fundamental that DPAs engage directly in dialogue and take the lead in providing the information, advice and support which will make a practical reality of data protection.[12]

The Privacy Commissioner already engages in similar activities under the current mandate under PIPEDA. Such education and outreach efforts are equally as important for the public sector and CIPL supports aligning the mandate of the revised Privacy Act with respect to research and education with the Privacy Commissioner's authority under PIPEDA to engage in such activities.

As Discussion Paper 4 rightly notes, including such a mandate within the Privacy Act "could support the Privacy Commissioner to proactively communicate to government institutions his interpretations and expectations about the requirements of the Act". Indeed, DPAs internationally, particularly in Europe, already engage in such education and outreach efforts at the public sector level. The General Data Protection Regulation (GDPR) applies to public and private sector organizations with negligible distinction and much of the guidance produced by European DPAs is equally relevant for public authorities and government institutions as it is for the private sector. Moreover, the European Data Protection Supervisor (EDPS), an independent supervisory authority is specifically tasked with ensuring that EU institutions and bodies respect data protection rules when processing personal information and developing new policies.

In that connection, we also recommend that the Privacy Act give the Privacy Commissioner the specific mandate to balance privacy with the ability of government to innovate and use personal information effectively. The Commissioner's role should encompass both facilitating the government's legitimate needs in collecting, using and sharing personal information and ensuring appropriate privacy protections for individuals. In other words, we suggest that modern data protection authorities must have the dual responsibility of enabling privacy as well as innovation and beneficial data use and that this should be made explicit in the Privacy Act.

**Q.4(b): Should a requirement to conduct a PIA be added to the Privacy Act? If so, is the current, policy-based "test" for when a PIA is required the most appropriate approach or are there other circumstances in which an institution should be legally required to undertake a PIA?**

CIPL strongly supports the risk-based approach to data protection and views risk assessment as one of the core elements of organizational accountability. As privacy risk is contextual, public sector organizations should understand and assess the risks to individuals of all their data uses. In that respect, CIPL supports

---

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf.

[12] *Id.* at page 30.

including a requirement to conduct a PIA in the revised version of the Privacy Act. However, the contours of this requirement must be carefully considered.

CIPL believes that public sector organizations should be required to conduct an initial high-level assessment of risk for any proposed data use. Such assessment could be aided by guidelines from the Treasury Board of Canada Secretariat and/or the OPC as to what might be high risk or low risk data uses, keeping in mind that such guidelines should be rebuttable by the results of the actual assessment. Only where likely high risks are identified and/or confirmed should public sector organizations have to perform a full-blown DPIA. Adopting such an approach would ensure:

- the requirement to conduct a PIA is built into the law in order to tackle the currently uneven approach of conducting PIAs across government institutions;
- a timely process for conducting and prioritizing the most important government PIAs by ensuring that more focus is placed on assessing and mitigating high risk processing activities; and
- the OPC spends time and resources reviewing only pertinent and truly risky processing activities.

With respect to the current policy-based test for when a PIA is required, CIPL believes the test should be construed more broadly. As drafted, the test seems to be confined to specific instances of processing around decision-making, changes to existing government programs and administrative purposes. However, government institutions might engage in processing operations outside of these areas that could be risky. Thus, rather than limiting the test to narrow and specific processing contexts, CIPL believes that the test should focus on likelihood and size of the risk proportionate to the benefits of the processing.

**Q.4(e): Is there a role for advance rulings or advisory opinions to supplement more general guidance from the OPC?**

CIPL believes that advance rulings and advisory opinions can provide a valuable tool for both government institutions to their ensure compliance with the Privacy Act and for the OPC in ensuring proactive privacy protection for individuals while advancing constructive engagement with the institutions it regulates.

The leadership function of DPAs places emphasis on ensuring as much constructive engagement as possible between DPAs and those they regulate. In practice, constructive engagement involves many different activities, including maximum consultation to foster a "no surprises" approach to oversight. By permitting the OPC to engage in advance rulings, organizations will be able to engage in beneficial dialogue with the Privacy Commissioner to understand what the right thing to do is in any given processing context when there are no common views or approaches, new requirements are at play or novel technology is involved. One step further along than general guidance on a topic, advance rulings facilitate proactive data protection compliance rather than after the fact corrective action by organizations.

Constructive engagement also involves creating a space for responsible innovation. Discussion Paper 4 notes that "an advance ruling or advisory opinion will provide guidance to regulated entities about how an oversight body would approach a particular legal issue if a complaint about that matter were received or if its oversight powers were otherwise engaged".[13] Internationally, several DPAs are providing similar

[13] *Supra* note 5 at page 5.

opinions to organizations via regulatory sandbox mechanisms whereby organizations are able to seek direction on specific projects that involve the processing of personal information and particularly complex data protection issues.[14] Although the exact structure and process for issuing advance rulings should be left to the legislature to decide in consultation with the OPC, regulatory sandboxes could provide one avenue for issuing such rulings.

Moreover, Discussion Paper 4 also notes that other federal public bodies in Canada have the ability to issue such advisory opinions, for instance, in the lobbying, competition and taxation sectors. Given the ever-increasing use of personal information by government institutions, CIPL strongly recommends providing the OPC with similar authority. Granting such authority is all the more supported by the fact that advance rulings are already possible at the provincial level (e.g. under Prince Edwards Island's Freedom of Information and Protection of Privacy Act).

**Complaint-handling**

**Q.4(g): Should the Privacy Commissioner have the discretion to decline to investigate a complaint? Under what circumstances?**

Yes, while the complaint-handling function of DPAs provides recourse for individuals and valuable insights for DPAs on data use and data protection practices, the role must not be given excessive priority over other functions of the Privacy Commissioner. Cases must be chosen carefully to prevent swamping the OPC with individual complaints that will drain its limited resources. As explained in our paper on Regulating for Results, CIPL believes that regulators should be able to concentrate on and prioritize more significant violations for enforcement, whose resolution will have the greatest impact on individuals and society.

In revising the Privacy Act, the Department of Justice Canada should consider the experience of European DPAs that have been inundated with complaints since the GDPR went into force. According to the EDPB, over 144,000 queries and complaints were made to European DPAs during the first year of the GDPR.[15] While there may be fewer complaints made to the OPC concerning government institutions versus private sector organizations, the OPC will need to consider the complaints it receives in the aggregate and as a result, the combined number of complaints may lead to swamping of the Privacy Commissioner if it does not have the discretion to decline to investigate complaints, particularly those that are frivolous or vexatious.

The approach of the UK ICO to addressing complaints, as described in Discussion Paper 4, provides a useful method of deciding which complaints to address and to what degree and could serve as inspiration in

[14] See, for example, the UK Information Commissioner's Office regulatory sandbox beta phase initiative, available at https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/; see also CIPL's white paper on "Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice", 8 March 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf for information about data protection sandboxes generally.

[15] See 1 Year GDPR – Taking Stock, European Data Protection Board, 22 May 2019, available at, https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en.

revising the Privacy Act. It should be for the OPC to decide which complaints merit a thorough investigation and accompanying investigation report through a combination of analyzing the complaints it receives, allocating its limited resources appropriately and prioritizing its regulatory objectives.

**Q.4(h): Should the Privacy Commissioner have the discretion to discontinue a complaint investigation or decline to prepare a comprehensive investigation report? If so, in what circumstances?**

CIPL believes that the Privacy Commissioner should have the discretion to discontinue an investigation or decline to prepare a comprehensive investigation report for the following reasons:

- The government institution in question may have remediated the issue and resolved the complaint that led to the investigation rendering the ongoing investigation moot;
- The OPC may have discovered that a complaint which looked meritorious on its face turned out to be frivolous or vexatious and no longer wishes to spend its limited resources investigating the complaint;
- The government institution may have made public statements outlining the reasons it was investigated by the OPC and the corrective actions it is now taking, rendering the issuing of a separate investigation report by the OPC pointless; and
- The OPC's investigation may have concluded that the government institution was in fact in compliance despite the complaint(s) made and as a result, the preparation of an investigative report is not necessary.

**Q.4(i): Should the Privacy Act be amended to require a complainant to first address their complaint to the government institution involved?**

Yes, CIPL believes that complainants should be encouraged to address a complaint initially to the government institution concerned, which, as an accountable organizations, should have complaint handling policies and procedures in place to deal with the complaint effectively. The government institution is best placed to actually remediate the issue at hand and will be able to provide much faster results than the OPC can. If the complaint at issue has merit and also impacts other individuals, the government institution and such other individuals have an interest in the government institution's learning about the complaint as quickly as possible and to take immediate action to eliminate or limit any harm. A requirement to first complain to the relevant government institution would also alleviate the burden on the Privacy Commissioner to deal with high volumes of complaints.

Furthermore, should the Privacy Act be amended to allow the OPC discretion to decline to investigate a complaint, as recommended above, then by going straight to the government institution involved, the complainant can ensure it has exhausted all avenues for recourse outside of the courts should the OPC decline to pursue the complaint as part of ensuring its overall regulatory effectiveness.

**Conclusion**

CIPL is grateful for the opportunity to participate in Justice Canada's Technical Engagement with Experts on the Modernization of Canada's Federal Privacy Act. We look forward to further opportunities for dialogue on the Privacy Act and Canada's efforts to revise and update its data protection regime generally.

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; or Sam Grogan, sgrogan@huntonAK.com.