

CHAPTER 6. SECURITY AND PRIVACY IMPLICATIONS OF E-PROCUREMENT IN THE TTIP

W. Gregory Voss

Professor of Business Law, Toulouse Business School (TBS)

Overview

Five years ago, the European Commission commented that electronic procurement (e-procurement) “is no longer a pipe-dream – it is increasingly a working reality in many regions and Member States” (European Commission, 2010). However, out of an EU public sector market for purchases of goods, services and works estimated at €2.4 trillion, e-procurement only accounts for between 5% and 10% of procurement, in spite of the potential savings of between 5% and 20% reported by entities that have made the switch to e-procurement (European Commission, 2012a). The United States has a similarly large government procurement market, worth \$1.7 trillion (GAO, 2015), and thus provides opportunities for the use of e-procurement and the extension of its potential benefits over a large base. Such huge markets should interest companies from the other side of the Atlantic. Yet the subject of security and privacy implications of e-procurement has not been raised by either the EU or the US in the resources that they have officially published (through the European Commission and the United States Trade Representative, respectively) to date regarding the TTIP negotiations.¹

As discussed in this article, the development of e-procurement is treated as a priority nationally, regionally and internationally, and e-procurement is seen as a way forward to increase efficiency and facilitate access to public tenders and increase transparency by “holding public authorities more accountable” (OECD, 2015). It is perceived as a means to enhance “value for money” through increased competition, reduced costs, and other related benefits (UN, 2011). The US e-government legislation called for work to ensure “effective implementation of electronic procurement initiatives”.² The European Commission has indicated the “strategic importance” of e-procurement, which ties in with the Digital Agenda for Europe and the e-Government Action Plan 2011-2015 (European Commission, 2012a). Furthermore, Europe has set out to develop e-procurement through recent revisions to its procurement directives, which it claims will increase the accessibility of businesses to procurement activity in the EU member states (European Commission, 2014). The recently revised EU procurement

1. See <http://ec.europa.eu/trade/policy/in-focus/ttip/> (last visited on August 2, 2015) (to date, no full negotiating text has been officially published by the EU on public procurement), and <https://ustr.gov/trade-agreements/free-trade-agreements/transatlantic-trade-and-investment-partnership-t-tip/t-tip-7> (last visited on August 2, 2015).
2. E-Government Act of 2002 (H. R. 2458) adding a new ch.36 (Management and Promotion of Electronic Government Services) to 44 U.S.C. of which §3602(12) on the Office of Electronic Government.

directives, currently in the process of transposition into member state national law, favour (and sometimes mandate) the use of “electronic means” in procurement in many instances (see, for example, Directive 2014/24/EU, which has a transposition deadline of April 18th 2016 (art. 90(1)). The importance of e-procurement was also highlighted in the preamble to the 2012 Revised Amendment to the World Trade Organization (WTO)’s 1994 Government Procurement Agreement (GPA 2012 Revision), which stresses the “importance of using, and encouraging the use of, electronic means for procurement” (WTO, GPA 2012 Revision, 2012). The current GPA 2012 Revision, however, provides only a very basic level of requirements regarding contracting using e-procurement, calling for the use of “generally available and interoperable” software “including those related to authentication and encryption” (WTO, GPA 2012 Revision, 2012, Art. IV. 3 (a)) and ensuring mechanisms establish the “prevention of inappropriate access” to systems (WTO, GPA 2012 Revision, 2012, Art. IV.3 (b)).

Recent EU trade agreements mirror procurement provisions in their government procurement chapters. This is the case with the Canada-EU trade agreement (CETA, 2014, Ch. X, Art. IV, 3. (a)-(b), p. 314, 1 August 2014 final version), and the EU agreements with members of the Andean Community, the EU agreement with Iraq, and the EU-Central American association agreement. Even earlier agreements, such as that between Chile and the EU, encourage the use of “electronic means of communication” and “electronic information systems”. If the EU and the United States are committed to achieving an ambitious outcome on procurement within the TTIP setting, the development of “GPA plus” provisions on e-procurement are essential in order to ensure security, privacy and confidentiality of information, together with the other benefits such as transparency and increased access that are provided by electronic means for providing tender information, communicating and transacting. For example, the European Commission reported on CETA that “Canada will also create a single electronic procurement website that combines information on all tenders and access to public procurement at all levels of government” (European Commission, 2013), and an equivalent mechanism may initially be provided for the parties to the TTIP so as to encourage market access for EU and US firms in each other’s markets.

The adoption of “GPA plus” elements under a TTIP framework could allow the EU and the US to “set a higher standard that could inspire a future GPA revision”,³ such as in the area of the security of e-procurement systems and platforms, all the while ensuring that security standards in this context, including requirements as to identity authentication, encryption, data storage and evidentiary elements regarding tenders (evidence of receipt and integrity of content) are set cooperatively, in a way that does not create artificial barriers to trade,⁴ thereby ensuring the access of Spanish and other European companies (and US ones, alike) to new markets. Such security standards, developed in collaboration, if set ambitiously using the partners’ combined expertise, could then become de facto “gold standards” internationally, because of the importance of the markets involved and the influence of these key players; they could serve as an inspiration for a future GPA revision and could influence other trade discussions in progress, such as TTP.⁵ As stated by Woolcock and Grier (2015):

3. European Commission, EU-US Transatlantic Trade and Investment Partnership: Public Procurement, Initial EU position paper, para. 2.1, p. 1.

4. See *id.*, para. 3.1, p.2, on the importance of ensuring that technical standards do not create artificial barriers.

...the TTIP could contribute to the international procurement arena by setting a new standard for procurement agreements. If the terms of the TTIP go beyond current procurement agreements, in particular, the GPA, it would likely provide the basis for the inclusion of its liberalisation of procurement in other agreements.... If the TTIP includes procurement rules that go beyond the revised GPA, they could provide the basis for incorporation in a subsequent revision of the GPA. Also, such new rules would likely be incorporated in any new FTAs that the EU and the US negotiate.

In this regard, it should also be noted that data security – the subject of GPA plus elements – is a key element of data protection and privacy, creating trust among parties.

The importance of security for trust, privacy and confidentiality in e-procurement

The security of the electronic means of e-procurement can have an impact on the trust that parties who use the system have in it, as has been aptly demonstrated in the private sector. This trust or "confidence" of entities is at the heart of the integrity of the procurement system and of transactions and is a prerequisite for the adoption of electronic market tools. In the private sector, in the case of e-commerce, this has been cited by the European Commission in its Digital Agenda. However, this is also true for public e-procurement systems as well. While there are phases of procurement, such as notification, submission, evaluation and ordering that are complex and need different treatment from that of the private sector (requiring "an agreed set of protocols and standards for organising the exchange of complex documents and interaction between the public purchaser and supplier"), there are many aspects of e-procurement that maybe applicable to and used by the B2B market, such as invoicing and payment after award (European Commission, 2010). Thus, some of the same concerns, such as that for security of the platform and of transactions, arise in the two cases. These concerns about security have been echoed in studies from academia (Khorana, Ferguson-Boucher, and Kerr, 2015) and the private sector (PWC, 2013). Trust is crucial; there must be confidence in both "government and the enabling technologies" and two themes that consistently appear in the literature in this regard, both regarding private sector marketplaces and e-government, are privacy and security (Carter and Bélanger, 2005).

At the same time, cybersecurity has recently been a critical concern, as evidenced by the European Commission's Cyber Security Strategy and Proposal for a Directive,⁶ and the White House's establishing of a Cyber Threat Intelligence Integration Center.⁷ This was also brought home in 2011, when the EU's Emissions Trading System (ETS) or so-called "cap and trade" market on carbon credits was hacked. The ETS suffered because "protections against crime, from background checks on carbon traders to basic Internet security to unified governance, were minimal from the start" (Funk, 2015). Potential hacking can interfere with transactions and communications and misappropriate data. This is a cautionary tale for the use of electronic means, the security of which could arguably better be managed at a higher level than the local one. Thus, common standards for encryption, electronic signatures, management of network identities and authorisations could be better handled.

5. See *id.*, para. 2.1, p. 1, on the impact of "GPA plus" elements on a future GPA revision.
6. See <https://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security>.
7. Press Release, The White House, Presidential Memorandum -- Establishment of the Cyber Threat Intelligence Integration Center, February 25 2015, available at <https://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat>.

In the e-procurement context the protection of security is synonymous with the protection of citizens' data privacy. The OECD (1993 amended 2013) states: "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data". Similarly, such protection helps ensure the confidentiality of Spanish and other private companies' proprietary information, whether in the tendering process or in the carrying out of government contracts, such as concessions or the provision of services.

The importance given to data protection in processing has already been shown by its inclusion in the 2014 revised EU procurement directives. There, data protection law must be taken into consideration when designing technical specifications, especially through the use of privacy by design in establishing specifications for the processing of personal data (see e.g. Directive 2014/24/EU, recital (77)). Similarly, the US Privacy Act of 1974, through its incorporation in the Federal Acquisition Regulation, applies to government contracting where a contractor designs, develops or operates a system of records on individuals.⁸ Such legislation, which is subject to "numerous exceptions" given wide interpretation, provides certain rights to data subjects, including, *inter alia*, a right to accuracy of data, allowing individual access for inspection, and certain information rights (Belanger and Hiller, 2006). Arguably, these are not as extensive as the rights provided by EU legislation, although a full comparative study is beyond the scope of this paper. Nonetheless, in the case of international standards, a high best level of data protection should be the one referred to in this design, regardless of differences otherwise existing between the legislation of the US and that of the EU in the matter. However, because of the differing levels of protection of personal data in the EU and the US, a common high level of protection may be a contested area in negotiations.

In addition to specific personal data or privacy legislation protections, the United States' Freedom of Information Act (FOIA) allows certain privacy exceptions to disclosure subject to FOIA requests for public records that include personal data or business trade secrets (Belanger and Hiller, 2006), although one would look to the Privacy Act for provisions regarding the sharing of documents between US government agencies. In the EU under the new procurement directives, access to certain documents and communications may need to be limited based on data protection principles (see e.g. Directive 2014/24/EU, art. 83(6) (on access to documents in enforcement actions) and art. 86(2) (on information exchange in administrative cooperation)). This is because access to such information may involve the processing of personal data subject to the requirements of EU data protection principles such as data minimisation, purpose limitation, relevance and security requirements, among others. As noted in the text of the procurement directives, EU data protection law applies (currently the 1995 Data Protection Directive (Directive 1995/46/EC), which will be repealed and replaced by the proposed General Data Protection Regulation once adopted), and the principle of data protection by design shall be taken into account when drawing up technical specifications relating to the processing of personal data (see e.g. Directive 2014/24/EU, recital 77).

Likewise, in the case that security is not ensured, the EU directives allow for reverting back to non-electronic means (see e.g. Directive 2014/24/EU, Art. 22(1)). Under the relevant provisions, if there is a breach of

8. See <http://www.gsa.gov/portal/content/104249> (last visited on August 2, 2015).

security or if electronic means cannot ensure the necessary security for extremely sensitive information, electronic means do not need to be used for communication in the submission process. This underscores the necessity of the highest level of security, for confidentiality and proprietary data protection, even where personal data is not involved.

In order to obtain such security in public procurement in a way that encourages transparency, efficiency and enhanced market access, this paper argues that there must be a coherent legal framework establishing rules and technical standards, and harmonisation of such technical standards. It should be noted that, related to the issues of privacy and confidentiality, the location of data stored in connection with procurement may be an issue in negotiations.

TTIP negotiations should address the issue of the use of cloud storage in the e-procurement context, information to be given to tenderers regarding the localisation of their personal data and trade secrets in the cloud and any national security or law enforcement legislation that may allow access to such data and secrets and the potential use thereof. The location of the data in terms of that of the hardware used to store it in the cloud at any given moment is important in determining the legal environment applicable to it (European Commission, 2012b), and this will have a bearing on law enforcement access to such data, an issue brought to light in connection with the NSA PRISM disclosures, which have been the subject of discussion in the context of current EU data protection law reform (Voss, 2014). Thus, this too may be a contested area for negotiations, as data privacy and cross-border data flows are considered contentious market access issues (Akhtar and Jones, 2014).

The TTIP: An opportunity to initiate a cooperative procedure to establish common rules?

EU-US discussions in the area of public procurement could provide for a formalised continuing set of discussions and actions to further advance protection of security, privacy and confidentiality in e-procurement through stages. In such a way, the negotiation of the TTIP could translate into a stellar opportunity for the EU and the US, through GPA plus elements, to set e-procurement standards for tomorrow, potentially inspiring a GPA revision in the future and having an impact on TTP negotiations, or the negotiation of other trade agreements to be entered into by the EU or the US.

However, any such advances may need to be conducted only on the central level to start with, especially given the US government argument that, "principles of federalism bar the federal government from compelling the states to open their procurement markets under an international agreement, such as the GPA" (Yukins, 2014). Nonetheless, the local levels should be targeted at a future time, as a means to reach "enhanced mutual access to public procurement markets at all administrative levels (national, regional and local)", identified by the council of the EU in its mandate for negotiations as one of its negotiating goals (Council of the European Union, 2013) and a means to bring true benefits to SMEs. It has been noted that countries with a "well implemented" e-procurement system "have noticed higher participation of SMEs ... due to

improved market access and a reduction in marketing costs" (UN, 2011). SMEs would have easier access to tender information available centrally online, and less paper bureaucracy with the various steps of the procurement process achievable online.

Furthermore, given the timeframe for TTIP negotiations, the most that one may likely expect to see in the eventually implemented agreement is the establishment of general undertakings and the initiation of actions for rule- and standard-making and to depend on a "living agreement" status for the further development of TTIP work on e-procurement following ratification.

There is some precedence for this as, following the GPA 2012 Revision a Bilateral Procurement Forum was established by the EU and the US to provide for ongoing dialogue (Woolcock and Grier, 2015). In addition, both parties adopted a "living agreement" procedure for government procurement in their recent free trade agreements (FTA) with the Republic of South Korea, for example, although not with specific tasks identified at the time of signature. In each case, a Government Procurement Working Group was established, which was able to deal with issues regarding government procurement subsequent to the entry into force of the FTA (see KORUS, 2010, art. 17.10 and KOREU, 2010, art. 15.3 (f), in accordance with art. 9.3). Moreover, CETA establishes a Committee on Government Procurement in order to further discussions with the goal of "affording Parties the opportunity to consult on any matters relating to the operation of this Chapter or the furtherance of its objectives, and to carry out such other responsibilities as may be assigned to it by the Parties" (CETA, 2014). Specifically, such a committee may promote activities that "may include information sessions in particular with a view to improving electronic access to publicly-available information on each Party's procurement regime, and initiatives to facilitate access for SMEs" (CETA, 2014, art. XIX (2) (d)), including those from Spain. However, what is being proposed in this paper goes further.

For example, on security matters, common rules on security and related common rules on interoperability and on confidentiality and privacy could be targeted. Moreover, such a task force could charge already existing agencies to represent the parties for some of their work. For example, in the area of security, the EU Agency for Network and Information Security (ENISA) could take this role for the European Union. Although ENISA is not a standards developing organisation itself, it "has been identifying and elaborating on the work performed by standardisation bodies (such as ISO, ETSI, ITU, CEN, CENELEC)" relevant to its work on network and information security standards development, sometimes through working collaboration, since 2009 (Purser, 2014). On the United States side, the National Institute of Standards and Technology, a standards and guideline-developing agency of the US Department of Commerce, could take the corresponding role.

More ambitiously, a choice of commonly approved platforms or common requirements for e-procurement platforms could be established. Having common systems would address the market fragmentation issue about which the European Commission has expressed concerns, "[market fragmentation] can emerge from the existence of a wide variety of systems, sometimes technically complex, [...] that can lead to increased costs for

economic operators/suppliers” (European Commission, 2012a). While the European Commission was speaking of intra-EU systems, when the transatlantic market is considered, this would be even truer, and some of the work of the EU on a regional basis may serve as a model for working internationally with the United States. Such developments arose cooperatively and not in competition and have the potential to impact the standards and policies of other nations in the area of e-procurement. This in turn would lead to greater transparency and access to markets through adoption of the e-procurement solution, through a cooperative process that would avoid a battle of standards and create efficiencies and protection for businesses (including SMEs) and citizens.

Establishing an e-procurement road map for the future

A first objective for negotiations, then, would be to recognise the benefits of e-procurement in the text of the TTIP and to obtain undertakings by the two partners to collaboratively develop security standards for e-procurement, dealing with the various issues identified in this paper. As part of such discussions, mutually acceptable e-procurement platforms could be identified or at least their relevant commonly required technical specifications could be established.

To begin with, the partners could each undertake to develop single window e-procurement portals, based on such security standards, which would centralise and make access to information easier. Single window e-procurement portals may be used by decentralised procurement systems, as they allow bidding to be conducted individually by contracting agencies and only require a system operating entity (UN, 2011). The EU and US should establish the TTIP as a “living agreement” and set up a working group tasked with developing the security standards mentioned above, and working toward additional centralisation, as discussed below.

Second, collaborative work between the US and EU could be initiated, with the working group tasked to aim at going further – initially determining the feasibility of the creation of a single international platform for public procurement to be used by the two partners. If determined to be feasible, the working group would be charged with working on its development. Such an achievement would fully ensure a single coherent framework, single technical infrastructure, efficiency and market access for economic actors from either side of the Atlantic. Such a platform should be scalable internationally, adopting the security standards already established. And why not host it in Spain?⁹ Although this last goal may today seem unrealistic, there have been cases of international web-based systems set up in the past, albeit in areas outside of government procurement.¹⁰

Third, establishing security standards for one platform and monitoring the implementation of these would obviously take fewer resources than doing so for numerous platforms based on various standards. Data protection and privacy protection should be easier to achieve. Costs for maintaining a platform would be reduced for governments, as they could be shared out through membership fees to the central international platform, and the increase in potential suppliers would drive down prices through com-

9. Spain already has experience with various e-procurement platforms. See e.g., <https://contrataciondelestado.es/wps/portal/plataforma> and https://contractaciopublica.gencat.cat/ecofin_pscp/AppJava/es_ES/search.pscp?reqCode=start.

10. These have been frequent in the B2B sector (in the automotive and aviation industries, as well as in finance), and certain researchers highlight the ability to compare e-procurement platforms to B2B web marketplaces (Assar and Boughzala, 2008).

petition. Having one set of terms and conditions and system requirements to comply with would help EU as well as Spanish businesses– especially SMEs– to trust that their confidential information and citizens’ data would be secured and protected, which would please both constituencies.

Conclusion

In conclusion, the TTIP could include provisions requiring work on the achievement of e-procurement in order to provide benefits to governments and market access to companies from both sides of the Atlantic. These should include the development of common security standards, the protection of data and privacy, centralised portals and, eventually, if feasible, an international platform. Here, what we are proposing is first incremental, but eventually leads to major steps. At each level the goal is clear – to increase confidence and trust in the e-procurement solution through enhanced security and (relatively) greater protection of privacy and confidentiality of information. And to do this in a way based on common best standards allowing Spanish and other SMEs one set of requirements with which to comply. The result should be greater public contract opportunities, more procurement competition, lower risk and higher benefits to consumers.

References

Akhtar, Shayerahllias and Jones, Vivian C. *Proposed Transatlantic Trade and Investment Partnership (T-TIP): In Brief*, Congressional Research Service Report R43158, June 11 2014.

Assar, Saïd and Boughzala, Imed. “Empirical evaluation of public e-procurement platforms in France”, *Int. J. Value Chain Management*, Vol. 2, No. 1 (2008), p. 90-108.

Bélanger, France and Hiller, Janine S. “A framework for e-government: privacy implications”, *Business Process Management Journal*, Vol. 12, Iss. 1 (2006), pp. 48-60.

Carter, Lemuria and Bélanger, France. “The utilization of e-government services: citizen trust, innovation and acceptance factors”. *Info. Systems J.* (2005) 15, 5–25.

Consolidated CETA Text (CETA), 21. Government Procurement, Art. XIX Institutions, September 25, 2014, para. 1 (online) <http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/ceta-aecg/text-texte/21.aspx?lang=eng>

Council of the European Union. *Directives for the negotiation on the Transatlantic Trade and Investment Partnership between the EU and the United States of America* (17 June 2013), ST 11103/13 RESTREINT UE/EU RESTRICTED.

Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC, 2014 O.J. (L 94) 65, 28 March 2014.

European Commission. *Green Paper on expanding the use of e-Procurement in the EU*, COM(2010) 571 final, 18 October 2010.

European Commission (2012a) *A strategy for e-procurement*, COM (2012) 179 final (20 April), available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0179:FIN:EN:PDF>

European Commission (2012b) *Unleashing the Potential of Cloud Computing in Europe*, COM(2012) 529 final, 27 September.

European Commission (2013) *Facts and figures of the EU-Canada Free Trade deal*, 18 October, available at: <http://trade.ec.europa.eu/doclib/press/index.cfm?id=974>

European Commission (2014) *Revision of Public procurement Directives – Frequently Asked Questions*, MEMO/14/20, 15 January.

Free Trade Agreement between the EU and its Member States, of the one part, and the Republic of Korea, of the other part (KOREU), 2011 O.J. (L 127/1) (14 May 2011), 16 September 2010 (effective 1 July 2011).

Free Trade Agreement between the United States of America and the Republic of Korea (KORUS), December 3, 2010 (effective March 15, 2012).

Funk, McKenzie. "The Hack that Warmed the World", *Foreign Policy*, January 30, 2015, available at: <http://foreignpolicy.com/2015/01/30/climate-change-hack-carbon-credit-black-dragon/>

Khorana, Sangeeta, Ferguson-Boucher, Kirsten and Kerr, William A. "Governance Issues in the EU's e-Procurement Framework", 53(2) *J. Common Market Studies* (2015), pp. 292-310.

OECD (1980, amended 2013) *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Sep. 23, 1980, as amended on July 11, 2013 by C(2013)79, annex, Part Two, 11. Security Safeguards Principle.

OECD. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, July 25 2002, 2002.

OECD. *Government at a Glance 2015*, OECD Publishing, Paris, 2015.

Price Waterhouse Cooper (PWC) *E-procurement: Golden Book of Good Practice*, European Commission Contract reference: MARKT/2011/097/C4/OP LOT2 Version: v1.3 (11 March 2013). (online) http://ec.europa.eu/dgs/internal_market/studies/docs/e-procurement-golden-book-of-good-practice_en.pdf

Purser, Steve. "Standards for Cyber Security". In: *Best Practices in Computer Network Defense: Incident Detection and Response*, M.E. Hathaway (ed.), IOS Press, 2014.

United Nations (UN). Department of Economic and Social Affairs, Division for Public Administration and Development Management,

E-Procurement: Towards Transparency and Efficiency in Public Service Delivery, Report of the Expert Group Meeting (4-5 October 2011).

United States Government Accountability Office (GAO). "The United States and European Union Are the Two Largest Markets Covered by Key Procurement-Related Agreements", Report to Congressional Requesters, *International Trade*, July 2015.

Voss, W. Gregory. "Looking at European Union Data Protection Law Reform through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later", 17(9) *J. Internet L.* 1, 12-24 (2014).

Woolcock, Steve and Grier, Jean Heilman. "Public Procurement in the Transatlantic Trade and Investment Partnership Negotiations", Paper No. 2 in the CEPS-CTR project *TTIP in the Balance* and *CEPS Special Report* No. 100 (February 2015).

World Trade Organization (WTO). Preamble, Revised Agreement on Government Procurement, Annex to the Protocol Amending the Agreement on Government Procurement (GPA 2012 Revision), adopted on 30 March 2012 (GPA/113).

Yukins, C. *The European Procurement Directives and The Transatlantic Trade & Investment Partnership (T-TIP): Advancing U.S. – European Trade and Cooperation in Procurement*, GW Law School Public Law and Legal Theory Paper No. 2014-15, GW Legal Studies Research Paper No. 2014-15 (2014). (online) <http://ssrn.com/abstract=2433219>