	Issue identified by	Details	Is this specific to 'thick' Whois?	If yes, has this also occurred in existing 'thick' gTLDs?	If yes, how has this been addressed?	Are additional measures recommended to address this issue?	If 'no' in column D, is there another effort addressing this issue or to which the information can be provided?
Privacy & Data Protection	NCUC	Requiring existing and future gTLD registries to provide thick Whois services would effectively bypass data privacy laws based on local legislation and jurisdictions.					
	NCUC	local registrars have collected the Whois data pursuant to their local privacy laws and speech protections. The movement of that that data, and ownership of that data, from a European, or Canadian, or Japanese, or Korean jurisdiction (among regions/countries with strong data protection laws) to another country (the US) raises enormous issues. This movement must be considered in light of the authority over the data that is being transferred, the possible/probable ownership of data that is being transferred, and the future implications of that transfer if/when ICANN rules on Whois data, service and protocol					
	NCUC	The requirements of thick Whois need privacy safeguards, because while some nations have laws in place to protect data, others have few or no laws at all.					
	NPOC	The key issue of access to data privacy is fundamentally linked to the fact that the data of the registrants is available publically through Whois queries. Whether this can be done through one, two or several databases contributes to magnify or not the problems, which by no means should be obviate, but we think that the primary focus (and worry) should first be on this "public access" feature of personal sensitive data regarding the registrants.					
	Verisign	Attention should be given where the migration from thin to thick could involve the transfer of large amounts of Personally Identifiable Information (PII) across jurisdictions. Consideration should be given to the protection and privacy of the Registrant in cases where having their PII publically available could constitute a risk to the Registrant as well as to the applicable registry and registrar as well as the increased risk to consumers; by making such PII publicly available, it could be misused to facilitate phishing and fraudulent activities.					