WIPEDRIVE ENTERPRISE

Why It Matters That WipeDrive's Source Code Has Never Left the USA

- **Trade secrets** are fully protected by US Law.
- **Code is accessed and maintained by US company employees**. Vindictive 3rd party employees are unable to insert malicious code into the codebase. Overseas coders do not face prosecution for malicious acts. [1]
- **Ensures full ownership of the WipeDrive IP**. There is no concern that the WipeDrive IP would be stuck in International IP Laws
- **No Transfer of Knowledge Capital.** Foreign coders can publish our competitor's code in their 'own' tool.
- **No User Data is accessible by 3rd party personnel.** The financial liability is costly if user data is leaked by overseas 3rd party staff.
- **Unknown security measures at foreign facilities** – Sony [2] is a prime example of hackers having physical access to facilities. Our USA facilities are secured and certified by NCSC.
- **3rd Party Firms outsource their work.** "Some Indian firms are sending managers to the large Chinese cities and outsourcing work there," says Marcella. "Unless I specifically state in the contract that the third-party provider can't re-outsource it, what's to keep them from outsourcing it to Beijing?" [3] Our competitor's may not have contracts that limit their 3rd party providers from outsourcing the coding to another, potentially risky, country.
- **Language/cultural translation** issues delay code releases and bug fixes.

For more information on data security and data erasure products, please contact WipeDrive at 801.224.8900.

Sources

1. https://siliconangle.com/2020/07/27/source-code-dozens-companies-including-nintendo-microsoft-adobe-published-online/
2. https://www.csoonline.com/article/2851649/hackers-suggest-they-had-physical-access-during-attack-on-sony-pictures.html
3. https://searchsecurity.techtarget.com/feature/The-security-costs-of-outsourcing-software-development