NYMITY
innovating compliance

Katie MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
PrivacyFramework@NIST.gov

14 January, 2019

Re: Developing a Privacy Framework (Docket No. 181101997-8997-01)

Dear Ms. MacFarland,

Nymity appreciates the opportunity to comment on the National Institute of Standards and Technology's ("NIST") recent request for information regarding the development of a privacy framework. Our comments seek to provide insight into how organizations around the world are currently managing enterprise wide privacy risk through the use of an existing, and widely-adopted, operational, outcome-focused privacy management accountability framework. Our comments will discuss the following:

- **Part 1: The Nymity Privacy Management Accountability Framework™ ("Nymity Framework") for Identifying and Mitigating Risk**
- **Part 2: Nymity Processing Purposs Risk Framework™**

About Nymity

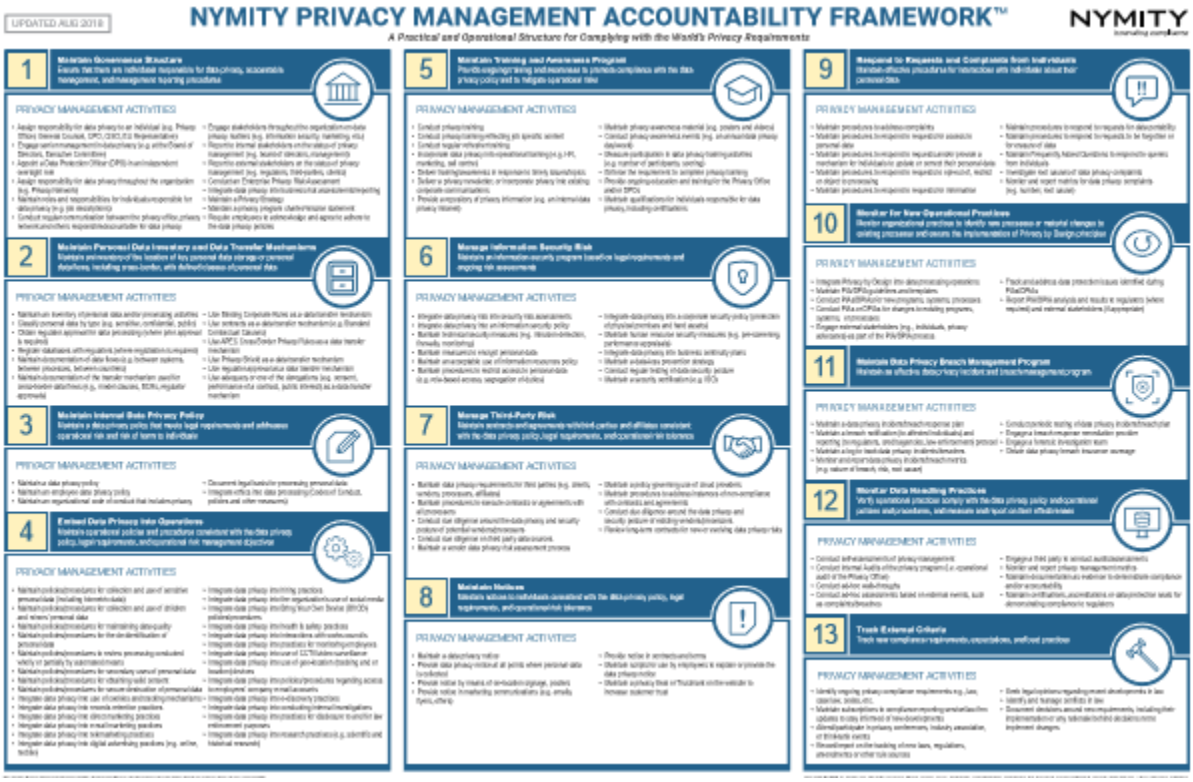
Nymity is a privacy research company providing research-based privacy management and compliance solutions to support the privacy office. For over 17 years, Nymity has helped thousands of privacy officers worldwide operationalize privacy management accountability and compliance and has helped organizations demonstrate compliance with 100's of privacy laws, frameworks, guidelines and regulations.

The area of "demonstrable privacy compliance and accountability" is one in which Nymity has done extensive research on both the concept and the implementation. In fact, Nymity has been conducting research since the notion of demonstrating accountability to a supervisory authority was first introduced in the 2009 Madrid Resolution[1]. In 2012 Nymity released the Nymity Privacy Management Accountability Framework™[2] and since that time, a host of other thought leadership around privacy management accountability and compliance which has been made available for free to the privacy community.[3]

[1] https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf
[2] https://www.nymity.com/data-privacy-resources/privacy-management-framework.aspx
[3] https://info.nymity.com/resources

Part 1: The Nymity Privacy Management Accountability Framework™ ("Nymity Framework") for Identifying and Mitigating Risk

Organizations around the world are operationalizing global privacy compliance and managing privacy risk through the Nymity Framework™ tool and effectively bridging the gap between and policies and principles and the implementation of practical and effective privacy management.



This image above is a thumbnail view of the Nymity Privacy Management Accountability Framework which is attached as Appendix A.

a. How was the Framework developed?

In 2002, Nymity began its research on accountability and building compliance solutions for individuals responsible for privacy within organizations. In 2009 Nymity enhanced this research through on-the-ground workshops around the world, including privacy and data protection regulators, examining what it would take for organizations to "demonstrate" accountability (e.g. internally to management or a board or externally to a regulator). Nymity's research revealed that no matter the industry or jurisdiction, privacy officers and other privacy leaders in organizations conduct many of the same activities. This led to the development of the Nymity Framework which was first released in 2012. It is made up of 13 Privacy Management Categories each containing multiple Privacy Management Activities (or technical and organisational measures), over 130 in total. ***It is a comprehensive, jurisdiction- and industry-neutral*** and works with privacy programs that are relatively new or very mature.

It was originally developed for communicating the status of the privacy program, in other words a framework for demonstrating accountability. It was designed to report on any privacy program, no matter how it is structured. For example, it works well with privacy programs structured around privacy principles, rationalized rules, standards and codes. 1000's of organizations around the world are using the framework to structure their privacy programs.

In 2015, the Nymity Framework was further enhanced with supporting tools after additional on the ground research with over 500 privacy officers across 20 countries and over 50 cities. It has been made available to the global privacy community for free and has become a recognized framework used for a variety of purposes. In fact, the Framework has been recognized as an international standard and is being taught as such at the Singapore Management University in an Advanced Certificate Program on Data Protection Frameworks and Standards.[4]

b. Privacy Management Activities are Supported by "Scopes"

Each of the 130+ privacy management activities are supported by a "scope" description to assist privacy officers in implementing and maintaining the activity. Example scopes are shown below and the entire scopes document is available for free through Nymity's resources.[5]

7. Manage Third-Party Risk

Maintain contracts and agreements with third parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance.

Maintain data privacy requirements for third parties (e.g., clients, vendors, processors, affiliates)

Data privacy laws continue to hold the organization accountable for protecting the privacy of any personal data accessed by third parties, including data processors, vendors, clients, and others who may receive personal data held by the organization. Thus, to be vigilant about data protection, the organization maintains internally template clauses of the data protection requirements that these third-parties must comply with.

Topics that may be addressed in the contracts include:

- Data protection responsibilities (e.g., acceptable use of personal data, use of subcontractors, restrictions on further disclosures or uses);
- Data security requirements;
- Data disposal at contract-end; and
- Breach response obligations.

Maintain procedures to execute contracts or agreements with all processors

This privacy management activity relates to maintaining procedures to execute contracts or agreements with all vendors processing personal information in the custody of an organization, including:

- Identification of vendor contracts which require specific privacy provisions;
- Alternatives for structuring the legal relationships involved so privity exists between all controllers and processors; and
- Considerations related to authority to execute such agreements.

This privacy management activity does not encompass the substantive privacy provisions which should be included in the contracts or agreements with data processors.

Conduct due diligence around the data privacy and security posture of potential vendors/processors

When selecting potential vendors/processors, the organization conducts an in-depth assessment of the third party's ability to perform the required activities in compliance with data protection laws and best practices. The third party's privacy and security posture are assessed to ensure it is capable of adhering to the organization's data privacy policy and information security policy (this could be through an audit conducted by the organization or a third party assurance report).

Conduct due diligence on third party data sources

Data protection/privacy laws and regulatory requirements continue to hold the organization accountable for protecting personal data under its control, regardless of the source of the data. To be vigilant about data protection/privacy and to ensure appropriate use of data acquired from 3rd party sources, it is important to conduct due diligence when procuring and utilizing externally sourced personal data. The level of due diligence will vary based on the geographic origin and sensitivity of personal data involved (I.e. Spain vs. US vs. Korea and Name, Address vs.

24

[4] https://academy.smu.edu.sg/index.php/data-protection-framework-and-standards-iso-29100-nymity-accountability-and-apec-privacy-framework

[5] Available at https://info.nymity.com/privacy-management-accountability-framework.

c. Is the Framework a "checklist" of privacy management requirements?

No. The Framework is not a one-size-fits-all approach and should not be implemented as such. It may be considered a "menu", not a checklist. Different sectors and individual organizations have different situations, needs and risk profiles and customize use of the Framework according to their unique needs and risks.

d. One Framework: Multiple Purposes

Although originally designed as a framework for demonstrating accountability, organizations around the world are using the Framework for multiple other purposes including:

- **Structuring the privacy program**: Some organizations, often those with a new privacy program or enhancing their existing program, have found the Nymity Framework effective for structuring the privacy program. The may use all 13 Privacy Management Categories or a subset. For example, a North American service provider/data processor many not implement many of the activities within certain Privacy Management Categories as they are not relevant given the nature of their data processing activities.

- **Baselining and planning**: Some organizations use the Nymity Framework as a checklist to identify existing Privacy Management Activities and for planning the implementation of new ones.

- **Benchmarking**: The Nymity Framework provides an effective mechanism to compare the privacy program across different areas of the organization, or between two organizations.

- **Regulatory Reporting**: Reporting to a regulator is a form of demonstrating accountability. Some organizations are using the Nymity Framework to show due diligence, for example in the event of a data breach to demonstrate that the event was an exception that occurred despite a robust program in place to prevent it, as opposed to a systemic issue.

- **Shifting Privacy Accountability to the Business:** Many privacy officers see the need to shift accountability to the business which in turn will allow the organization to cover more risk and incorporate privacy by design throughout the organization. The Nymity Framework is used as a structure to ensure the creation and maintenance of "accountability mechanisms" which ultimately empower the business, and ongoing compliance and monitoring of the program. Using the foundation of existing global policies and guidelines that address regulatory requirements, the Nymity Framework is used as a tool to make sure there are *procedures, work instructions and guidelines that could be leveraged more globally and in a more scalable, regulatory agnostic and efficient way for the organization.* [6]

[6] As discussed in Nymity's Publication, "From Privacy Project to Privacy Program: Leveraging GDPR Compliance Initiatives to Create One Accountable Privacy Program in Order to Comply with Multiple Laws" found at https://info.nymity.com/from-privacy-project-to-privacy-program-whitepaper. Co-authored by Jennie Hargrove, HID Global, Michael Scuvee, Coca-Cola European Partners and Alexys Carlton, Otter Products and Blue Ocean Enterprises.

- **Converting One-Time Compliance Projects into Sustainable Business Operations:** Considering the European GDPR[7] compliance efforts as an example, in practice, many companies organized their GDPR project into work packages in order to implement the requirements (whether it is in strategy, assigning responsibilities for the new controls, creating records of processing activities or revisiting notices, policies and procedures). The adoption of the Nymity Framework makes it easy to identify a stable and natural home for the controls resulting from work packages and deliverables of a GDPR project.[8]

- **Prioritizing Investments and Justifying Budgets:** The Nymity Framework helps organizations determine which privacy management activities are most important to assure risk management, privacy compliance and accountability. In turn, this helps organizations justify the prioritization on investments and maximize resources

- **Communicating Privacy and Risk:** The Nymity Framework provides a common language for privacy management within the organization. This improves understanding among various departments including in IT, operational and functional units such as IT, HR and marketing. It also serves in reporting the status of the privacy program to the Board and other key stakeholders .

- **Auditing and Assessing:** The Nymity Framework is also used by organizations to audit and assess privacy management throughout the organization.

e. Nymity Framework Mapping to Comply with Multiple Laws, Frameworks and Other Privacy Obligations

The Nymity Framework has been mapped to over 800 privacy laws, international privacy frameworks, guidelines and regulations from around the world and serves as one framework resulting in compliance with multiple obligations. Below is a thumbnail view of a selection of obligation requirements that have been mapped the Nymity Framework and this selection is available in its entirety in Appendix B.

Mapping a multitude of privacy obligations to the Nymity Framework has been invaluable to organizations in bridging the gap between policies and procedures and one accountable, efficient, scalable and repeatable privacy management program.

---

[7] Regulation EU 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

[8] As discussed in Nymity's Publication, "From Privacy Project to Privacy Program: Leveraging GDPR Compliance Initiatives to Create One Accountable Privacy Program in Order to Comply with Multiple Laws" found at https://info.nymity.com/from-privacy-project-to-privacy-program-whitepaper. Co-authored by Jennie Hargrove, HID Global, Michael Scuvee, Coca-Cola European Partners and Alexys Carlton, Otter Products and Blue Ocean Enterprises.

Nymity Privacy Management Accountabilty Framework - Sample Mapping									
Privacy Management Categories and Associated Privacy Management and Activities	GDPR	California Consumer Privacy Act 2018	Brazil LGPD	Canadian Guidance (Getting Accountability Right with a Privacy Management Program published by Office of Privacy Commissioner 2012)	Privacy Management Program (PMP) and Best Practice Guide (Hong Kong)	OECD Privacy Framework	General Accepted Privacy Principles (GAPP)	APEC Cross Border Privacy Rules	EU US Privacy Shield
Explanatory Notes: The mapping is based on which privacy management activity would provide evidence of the obligation set out in the rule source. In cases where an obligation is conditional (i.e., if organization does x, then y obligations result), these are tagged to PMAs. Where there is an exemption (e.g., if x is the case, then the organization does not need to comply), these are not tagged to any PMAs.									
Maintain Governance Structure									
Assign responsibility for data privacy to an individual (e.g. Privacy Officer, General Counsel, CPO, CISO, EU Representative)	Article 27				A. 1 (b)	x (14, 15)	x (1.1.2, 1.2.8)	Mandatory (Accountability 40)	
Engage senior management in data privacy (e.g. at the Board of Directors, Executive Committee)				A.1.a, A.1.b	Yes A. 1 (a)	x (14, 15)	x (1.1.2)		
Appoint a Data Protection Officer/Official (DPO) in an independent oversight role	Articles 37, 38		Article 41						
Assign responsibility for data privacy throughout the organization (e.g. Privacy Network)			Article 50	Yes A.1.c		x			
Maintain roles and responsibilities for individuals responsible for data privacy (e.g. Job descriptions)	Article 39			Yes A.1.a, A.1.b	Yes A.1.a, A.1.b		x (1.2.9)		
Conduct regular communication between the privacy office, privacy network, and others responsible/accountable for data privacy	Article 38			Yes A.1.b	Yes A.1.b				
Engage stakeholders throughout the organization on data privacy matters (e.g., information security, marketing, etc.)				Yes A.1.d	Yes A.1.c				
Report to internal stakeholders on the status of privacy management (e.g. board of directors, management)				Yes A.1.a, A.1.d	A. 1 c		x (1.1.2; 1.2.1)		
Report to external stakeholders on the status of privacy management (e.g., regulators, third-parties, clients)						x (15(a)(iv)) (original explanatory memo of para 12. Openness?)			
Conduct an Enterprise Privacy Risk Assessment	Articles 39, 24		Article 50	Yes A.2.c		x (15(a)(iii) and explanatory memo)	x (1.2.4)		
Integrate data privacy into business risk assessments/reporting				Yes A.2.c	A 1				
Maintain a Privacy Strategy									
Maintain a privacy program charter/mission statement									
Require employees to acknowledge and agree to adhere to the data privacy policies				Yes A.2.b			x (1.1.1)		

Part 2: Nymity Processing Purposes Risk Framework™

The GDPR is considered a risk-based regulation. This means, in part, that organizations must take extra steps to identify likely high risk processing prior to the processing and conduct a risk assessment. Article 35 (Data protection impact assessments) of the GDPR states that:

> (1) where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, *is likely to result in a high risk to the rights and freedoms of natural persons*, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.[9]

In connection with this requirement, and to support organizations in identifying high-risk, Nymity conducted extensive research in order to help companies in identifying likely high risk. One of the main measures of high risk relates to the purposes of processing personal data. Nymity's research identified a comprehensive list of purposes of processing that has been categorized in order to create a processing purposes risk Framework. The Framework is included here.

[9] Article 35(1) Regulation EU 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

Likely - aspects of the type of data processing may pose or threaten to cause significant harm to individuals
Unlikely - the type of data processing is unlikely to pose a threat of harm to individuals
Conditionally - the data processing may pose or threaten to cause harm if certain conditions are met

Processing Purposes Risk Framework™

Brand Promotion and Maintenance	
Carry out fundraising for charitable purposes	Unknown
Communicate developments / updates to customers	Conditional
Conduct focus groups and consultations	Unknown
Conduct opinion analysis	Likely
Conduct public relations activities	Unknown
Develop and implement crisis communication plans	Unknown
Engage in investor relations	Unknown
Manage events / press conferences	Unlikely
Manage the company website and social media presence	Conditional
Manage user communities	Conditional
Monitor queues at call centers	Conditional
Obtain customer / user feedback	Unknown
Publicly address customer complaints	Likely
Report diversity statistics	Unknown
Respond to inquiries/requests from customers	Unknown
Solicit and publish endorsements	Unknown
Business Intelligence	
Plan strategy and growth	Unlikely
Build a data warehouse	Conditional
Build a report for a business function	Unknown
Create a new business function database	Unknown
Implement a new BI visualization tool	Conditional
Company Finances	
Plan strategy and growth	Unlikely
Manage accounts payable	Unlikely
Manage accounts receivable	Unlikely
Manage credit accounts	Unknown
Process payment through insurance coverage	Conditional
Company Policy Compliance	
Conduct Internal Audits	Unlikely
Manage corporate expenses	Unlikely
Manage employee expenses	Unlikely
Monitor for possible corruption or unethical practices	Unknown
Reimburse expenses	Unlikely

Compensation and Benefits	
Administer bonus / recognition program	Likely
Administer company car program	Unknown
Administer Employee Assistance Program (EAP)	Likely
Administer employee health/dental/vision benefits	Unknown
Administer employee retirement savings program	Unknown
Administer long/short term disability program	Likely
Create equitable and competitive pay levels	Conditional
Direct deposit paycheque into bank account	Unlikely
Issue paycheques/administer payroll	Unlikely
Maintain a record evidencing payments	Unlikely
Manage cafeteria/store for employees	Unknown
Manage retirement benefits	Unknown
Provide a space for nursing mothers	Unknown
Provide daycare	Unknown
Provide flexible work arrangements	Unknown
Provide reimbursement for public transit	Unknown
Provide special offers/discounts from third parties	Conditional
Provide tuition assistance	Unknown
Report to domestic tax authorities	Unlikely
Consumer Profiling	
Administer loyalty programs	Likely
Advise customers on investment strategies	Likely
Advise customers on philanthropy	Unknown
Advise customers on retirement planning	Likely
Advise customers on tax strategies	Unknown
Advise customers on trust and estate planning	Unknown
Conduct focus groups and consultations	Unknown
Conduct marketing analytics	Likely
Create consumer profiles based on data broker/third party data	Likely
Forecast Likely Future Behavior based on Predictive Technologies	Likely
Measure audiences for a specific market	Likely
Obtain customer / user feedback	Unknown
Offer a mobile application	Conditional
Offer financial products based on consumer profiles	Unknown
Set Insurance Premiums Based on Customer Profile	Likely
Track app usage	Likely
Track location behaviour (mobile)	Likely
Track online behaviour (websites)	Likely

Current employee relationship	
Administer employee directory	Unknown
Conduct drug screening	Likely
Conduct Medical Screening	Likely
Coordinate employee travel	Unlikely
Deliver training and development	Unlikely
Determine eligibility for and provide accomodation	Likely
Identify skills	Conditional
Identify training needs	Conditional
Maintain a disaster/pandemic reporting plan	Unknown
Maintain current employment records	Unlikely
Make reasonable accommodation for employees with disabilities	Unlikely
Manage conflicts between employees	Unknown
Manage corporate expenses	Unlikely
Manage leave programs	Unlikely
Manage relationships with trade unions and works councils	Unlikely
Offer a mobile application	Conditional
Onboard/offboard employees	Unlikely
Populate employee profile by importing existing data from other databases	Conditional
Provide references	Unknown
Reimburse expenses	Unlikely
Track sick day/vacation entitlement	Unlikely
Track time and attendance	Conditional
Customer Profitability	
Develop conduct and risk models	Likely
Manage customer profiles	Likely
Measure Return on Customer	Unknown
Measure sales force effectiveness and funnel management	Unknown
Plan and forecast sales	Unknown
Track conversion actions	Unknown
Customer Support	
Administer warranty program	Unknown
Help customers complete transactions	Unknown
Manage user communities	Conditional
Monitor queues at call centers	Conditional
Offer a mobile application	Conditional
Respond to inquiries/requests from customers	Unknown
Route planning for deliveries	Conditional
Schedule appointments and send reminders	Unknown
Track service/maintenance checks or repairs	Likely
Verify identity / authorization of user	Unknown

Customer/User Satisfaction	
Communicate developments / updates to customers	Conditional
Maintain Automatic Banking Machines	Unknown
Manage customer / user complaints	Unknown
Manage customer profiles	Likely
Manage Online Banking Systems and Applications	Unknown
Manage Telephone Banking Systems and Applications	Unknown
Obtain customer / user feedback	Unknown
Personalize customer interfaces	Conditional
Process returns	Unlikely
Provide user control over their personal data and communication preferences	Unknown
Show customer appreciation	Unknown
Employee Engagement	
Administer employee giving/matching gifts program	Unlikely
Administer employee retention program	Unknown
Administer health and wellness program	Likely
Assess employee satisfaction	Conditional
Facilitate charity events and participation	Unknown
Facilitate Corporate Communications and Collaboration	Unknown
Facilitate diversity and inclusion groups	Conditional
Facilitate volunteer activities	Unknown
Optimize the corporate intranet using analytics	Conditional
Publish employee newsletters / brochures	Unknown
Employee Performance	
Conduct performance appraisals	Likely
Investigate instances of noncompliance and manage disciplinary actions	Likely
Manage conflicts of interest	Unknown
Manage disciplinary actions for instances of noncompliance	Unknown
Manage employee complaints / reports of misconduct	Conditional
Manage whistleblower program	Conditional
Monitor email	Likely
Monitor employees through video surveillance (e.g. CCTV) systems	Likely
Monitor job performance	Likely
Monitor online behaviour	Likely
Monitor use of electronic assets/tools	Likely
Support career/leadership development	Unlikely
Track employee behaviour outside of the workplace	Likely
Track time and attendance	Unlikely
Former Employee Relationship	
Maintain records of former employees	Unlikely
Manage alumni network	Unknown
Manage retirement benefits	Unlikely
Provide references	Unknown

Health and Safety	
Conduct drug screening	Likely
Conduct Medical Screening	Likely
Employ security guards	Unknown
Evaluate and remediate safety / accessibility issues	Unknown
Gather evidence through video surveillance (e.g., CCTV) systems	Likely
Investigate security incidents	Unknown
Maintain a blacklist	Likely
Maintain emergency contact details	Unknown
Maintain employee emergency contact details	Unlikely
Monitor employee location for security purposes	Likely
Provide a staff nurse & sick room facilities	Likely
Report workplace safety incidents	Unlikely
IT Services	
Change or implement business systems / applications / processes	Likely
Consolidate systems & servers	Likely
Manage hardware and devices	Unlikely
Manage software and applications	Unlikely
Manage telecom and Internet networks	Conditional
Provide and manage electronic communication interfaces (e.g. EDI, API, etc.)	Conditional
Provide email accounts, IM, Voice Mail, Phone	Unlikely
Provide IT Support	Unknown
Test products, systems, applications	Unknown
Lead Generation	
Conduct competitions for consumers	Unknown
Gather data about potential leads from data brokers/third parties	Likely
Gather data about potential leads from individuals	Conditional
Gather data about potential leads from public sources	Likely
Gather data about potential leads from user friends and contact lists	Likely
Maximize customer database for upselling and cross-selling	Likely
Nurture and Manage the Relationship	Unknown
Profiling for leads	Likely
Legal Claims/Defense	
Enforce IP Rights	Conditional
Gather evidence through video surveillance (e.g., CCTV) systems	Likely
Manage arbitration, litigation or similar proceedings	Unlikely
Manage litigation holds	Unlikely
Prepare briefs, submissions, or other documentation for courts and tribunals	Unlikely
Respond to discovery requests	Unlikely
Legal/Regulatory Compliance	
Analyze adverse events report for patterns	Conditional
Comply with securities/governance requirements and standards	Unlikely

Conduct assessments for driving, workplace injuries, ability to care for oneself to government agencies	Conditional
Conduct Internal Audits	Unlikely
Conduct Know-Your-Client (KYC) Procedures	Likely
Detect IP rights violations/theft of IP	Conditional
Fulfill licensing obligations	Unknown
Maintain compliance with industry watch-lists	Likely
Manage company shareholder records	Unlikely
Manage legal formalities/reporting requirements of subsidiaries	Unlikely
Manage whistleblower program	Conditional
Monitor for possible corruption or unethical practices	Unknown
Monitor transactions for Anti-Money-Laundering Compliance	Likely
Monitor transactions for Identity Theft Red Flags	Likely
Receive adverse event information	Conditional
Report adverse events	Conditional
Report assessments for driving, workplace injuries, ability to care for oneself to government agencies	Conditional
Report Potential Domestic Abuse to Authorities	Unknown
Report Potential Elder Abuse to Authorities	Unknown
Report to counter-terrorism authorities	Unknown
Report to Credit Reporting Agencies	Unknown
Report to domestic tax authorities	Unlikely
Report to foreign tax authorities	Unlikely
Report to public health agencies and centers for disease control	Unknown
Respond to discovery requests	Unknown
Respond to law enforcement requests	Unknown
Screen for economic sanctions and export controls	Unknown
Support Board of Directors operations	Unknown
Mergers, Acquisitions and/or Restructuring	
Acquire a company or part of a company	Conditional
Execute a reorganization	Unknown
Integrate databases following a merger/acquisition	Likely
Merge or consolidate the company or part of the company	Conditional
Perform due diligence on potential acquisitions	Unknown
Sell the company or part of the company	Unknown
Monitoring Customer Interactions	
Assess current procedures for effectiveness	Likely
Identify reputational or operational risks	Likely
Manage quality of customer support interactions	Likely
Recall defective products	Conditional

Procurement	
Assess conflicts of interest	Unknown
Assess Requests for Proposals (RFPs)	Unknown
Audit suppliers/vendors	Unknown
Conduct background screens on vendor staff	Likely
Conduct ongoing due diligence	Unknown
Conduct supplier screening/due diligence	Unknown
Eliminate possible corruption or unethical practices	Unknown
Investigate instances of vendor noncompliance	Unknown
Manage supplier performance/quality	Unknown
Supply chain management	Unknown
Track purchase orders and issue payments	Unlikely
Product/Service Provision	
Automate the application process for products and services	Unknown
Conduct Credit Checks to Determine Eligibility for Products/Services	Conditional
Deploy new products and services to market	Unknown
Develop financial or credit risk models	Likely
Enable ongoing/repeatable payments for products/services	Unknown
Fulfill licensing obligations	Likely
Generate profit from licensing personal data databases to third parties	Conditional
Generate profit from sales of personal data to third parties	Conditional
Issue invoices	Unknown
Issue Quotes and Proposals	Unknown
Process data on behalf of another organization	Unknown
Process one-time payments for products / services	Unknown
Provide and Manage telecom and Internet services	Likely
Provide reports to third party content owners	Likely
Publish Online or Print Content	Unknown
Reduce customer churn	Conditional
Remind customers when prescriptions need refills	Conditional
Report aggregate analytics data to third parties	Likely
Schedule appointments and send reminders	Unknown
Ship / deliver products / services	Unknown
Verify identity / authorization of user	Unknown
Promote Products/Services	
Administer loyalty programs	Likely
Conduct B2B marketing campaigns	Unlikely
Conduct digital marketing campaigns	Likely
Conduct direct mail marketing campaigns	Conditional
Conduct direct to healthcare professional marketing	Conditional
Conduct email marketing campaigns	Likely
Conduct focus groups and consultations	Unknown
Conduct outbound telemarketing activities	Conditional
Conduct SMS marketing campaigns	Conditional

Gather data from data brokers/third parties to send promotional communications	Likely
Measure ad performance	Likely
Participate in affiliate / partnership programs	Likely
Personalize and target marketing activities	Likely
Personalize websites	Conditional
Publish newsletters	Unlikely
Send location-based marketing	Likely
Solicit and publish endorsements	Unknown
Track ad conversion	Likely
Protect/Manage Company Assets	
Conduct exit bag checks	Likely
Escort terminated employees off the premises	Unknown
Gather evidence through video surveillance (e.g., CCTV) systems	Likely
Identity Access Management (IAM)	Unlikely
Manage access via badge/fob system	Unlikely
Manage access via biometric authentication	Likely
Manage Bring Your Own Device (BYOD) Program	Likely
Manage real estate holdings and leases	Unknown
Manage security of data on devices during border crossings	Unknown
Manage security of the intranet	Conditional
Manage visitor access	Unlikely
Manage website security	Conditional
Monitor network activity	Likely
Protect systems, network, infrastructure and computers	Conditional
Scan network traffic for malicious activity	Conditional
Scan network traffic to stop data exfiltration	Conditional
Securely destroy data	Unknown
Track physical assets	Likely
Records Management	
Establish a repository for preservation and research use	Likely
Establish and review documenting records systems	Likely
Identify records to be preserved for historical and research purposes	Unlikely
Maintain operational efficiency by controlling the volume of records	Unknown
Maintain transaction records	Unlikely
Manage the changeover from paper to electronic records management systems	Likely
Preserve corporate memory and heritage	Unknown
Provide efficient access to the right information	Unknown
Respond to information enquiries	Unknown
Securely destroy data	Unknown
Standardise information sources throughout an organization or group of organizations	Unknown

Recruitment	
Conduct Credit Checks	Likely
Conduct criminal background checks	Likely
Conduct drug screening	Likely
Conduct education/credentials checks	Likely
Conduct interviews	Unlikely
Conduct Medical Screening	Likely
Conduct or attend recruiting events	Unlikely
Conduct psychometric and personality tests	Likely
Conduct reference checks	Likely
Gather data about candidates in response to job postings	Unlikely
Identify and attract qualified candidates through resume and job posting websites	Unlikely
Identify and attract qualified candidates through social media	Likely
Offer a mobile application	Conditional
Report diversity statistics	Unknown
Verify identity	Unknown
Verify right to work	Unknown

Research & Development	
Aggregate data to facilitate analytics	Conditional
Analyze drug efficacy, conduct pharmacovigilance	Likely
Build a new product or service	Conditional
Carry out fundraising for R&D	Unknown
Collaborate with field experts or professionals on product testing/evaluation	Unknown
Conduct clinical trials	Likely
Conduct focus groups and consultations	Unknown
Conduct opinion analysis	Likely
Conduct product health and safety risk assessments	Unknown
Create structured data from unstructured sources	Likely
Deploy fixes/updates to products	Unknown
Ensure product and user security	Conditional
Identify candidates for clinical trials	Likely
Measure audiences for a specific market	Likely
Monitor clinical trial group results	Likely
Monitor clinical trial results / impact on participants	Likely
Offer a mobile application	Conditional
Offer online products or services	Unknown
Test products, systems, applications	Unknown
Track product performance	Likely
Track use of products / services	Likely
Troubleshoot bugs	Unknown
Use consumer insights in product design	Unknown

Use third party application programmer interfaces (APIs) in app development	Conditional
Workforce Planning	
Administer employee retention program	Unknown
Create succession plans	Unknown
Engage in project management activities	Unknown
Engage non-permanent personnel	Unknown
Organize the work of individuals and work groups	Unknown
Plan and forecast workforce requirements	Unknown
Plan and use the workspace	Unknown
Relocate employees	Unknown
Support talent management	Unknown
Track data related to Affirmative Action & Equal Employment Opportunity programs	Unknown
Store layout & merchandise planning	
Conduct Simulations and Analyze Virtual Shoppers	Likely
Forecast Likely Future Behavior Based on Predictive Technologies	Likely
Measure audiences for a specific market	Likely
Operate recommendation engines	Likely
Track customer traffic patterns	Likely
Understand consumer shopping habits	Likely
Fraud/Loss Prevention and Detection	
Detect Fraudulent Claims Based on Analyzing Patterns in Claims Histories	Likely
Implement a fraud/loss prevention system/workflow	Unknown
Investigate insurance claims	Likely
Monitor beneficiaries	Likely
Monitor transactions for Fraud Prevention	Likely
Predict future fraudulent claims based on analyzing patterns in claims histories	Likely
Financial Products, Investments and Insurance	
Administer Insurance Policies	Likely
Conduct Credit Checks to Determine Eligibility for Financial Products	Likely
Conduct Medical Screening for Insurance Purposes	Likely
Execute wills, act as power of attorney	Unknown
Invest on behalf of customers	Unknown
Manage bankruptcy proceedings	Unknown
Process Insurance Claims	Likely
Provide and manage annuities	Unknown
Provide and manage auto loans and other secured loans	Likely
Provide and manage chequing and savings accounts	Conditional
Provide and manage credit cards	Likely
Provide and manage debt resolution services	Likely
Provide and manage electronic payments	Likely
Provide and manage international payments/transfers	Likely

Use third party application programmer interfaces (APIs) in app development	Conditional
Workforce Planning	
Administer employee retention program	Unknown
Create succession plans	Unknown
Engage in project management activities	Unknown
Engage non-permanent personnel	Unknown
Organize the work of individuals and work groups	Unknown
Plan and forecast workforce requirements	Unknown
Plan and use the workspace	Unknown
Relocate employees	Unknown
Support talent management	Unknown
Track data related to Affirmative Action & Equal Employment Opportunity programs	Unknown
Store layout & merchandise planning	
Conduct Simulations and Analyze Virtual Shoppers	Likely
Forecast Likely Future Behavior Based on Predictive Technologies	Likely
Measure audiences for a specific market	Likely
Operate recommendation engines	Likely
Track customer traffic patterns	Likely
Understand consumer shopping habits	Likely
Fraud/Loss Prevention and Detection	
Detect Fraudulent Claims Based on Analyzing Patterns in Claims Histories	Likely
Implement a fraud/loss prevention system/workflow	Unknown
Investigate insurance claims	Likely
Monitor beneficiaries	Likely
Monitor transactions for Fraud Prevention	Likely
Predict future fraudulent claims based on analyzing patterns in claims histories	Likely
Financial Products, Investments and Insurance	
Administer Insurance Policies	Likely
Conduct Credit Checks to Determine Eligibility for Financial Products	Likely
Conduct Medical Screening for Insurance Purposes	Likely
Execute wills, act as power of attorney	Unknown
Invest on behalf of customers	Unknown
Manage bankruptcy proceedings	Unknown
Process Insurance Claims	Likely
Provide and manage annuities	Unknown
Provide and manage auto loans and other secured loans	Likely
Provide and manage chequing and savings accounts	Conditional
Provide and manage credit cards	Likely
Provide and manage debt resolution services	Likely
Provide and manage electronic payments	Likely
Provide and manage international payments/transfers	Likely

Provide and manage investment products	Conditional
Provide and manage loans and lines of credit	Likely
Provide and manage mortgages	Likely
Provide and manage offshore accounts	Conditional
Provide and manage registered savings plans	Unknown
Provide and manage retirement savings accounts	Unknown
Provide and manage safety deposit boxes	Unknown
Provide and manage student loans	Likely
Provide and manage student/youth accounts	Unknown
Provide and manage trusts and estates	Likely
Provide auto insurance	Likely
Provide health insurance	Likely
Provide life insurace	Likely
Provide long term disability and critical illness insurance	Likely
Provide mortgage and loan insurance	Likely
Provide property insurance	Likely
Provide reinsurance	Likely
Provide travel insurance	Likely
Set Insurance Premiums Based on Customer Profile	Likely
Underwrite Insurance Policies	Likely
Health Care, Treatment and Support	
Conduct healthcare tests	Conditional
Conduct medical/diagnostic imaging	Conditional
Dispense medicine	Conditional
Interpret healthcare test results	Conditional
Issue test requisitions	Conditional
Manage patient communities	Likely
Provide and manage medical devices	Likely
Provide and manage organ and tissue donation	Likely
Provide and manage smart pills (ingestables that release medicine and relay patient data)	Likely
Provide chaplaincy services	Conditional
Provide curative care	Conditional
Provide fitness devices	Likely
Provide genetic counselling	Likely
Provide healthcare test results - Patient Care	Conditional
Provide outpatient services	Conditional
Provide palliative care	Conditional
Provide preventive care	Conditional
Provide referrals	Conditional
Provide rehabilitative services	Conditional
Provide second opinions	Conditional
Review and reconcile drug prescriptions and dosages	Conditional

Track consumption of medicine	Likely
Verify identity / authorization of patient	Unknown
Quality Healthcare	
Assess quality of care	Conditional
Conduct mortality or serious incident reviews	Conditional
Manage health IT systems	Likely
Provide and manage electronic health records (EHRs)	Likely
Provide and manage medical devices	Likely
Provide and manage personal health records (PHRs)	Likely
Provide referrals	Conditional
Provide second opinions	Conditional

Concluding Comments

Nymity appreciates the opportunity to provide comments for this initiative and appreciate NIST's engagement with the global privacy community. We look forward to continuing to work with your office throughout this process.

Terry McQuay
President and Founder
Nymity, Inc.

Teresa Troester-Falk
Chief Global Privacy Strategist,
Nymity, Inc.