

U.S. Department of Commerce U.S. Patent and Trademark Office



Privacy Impact Assessment for the DesignVision (DV)

Reviewed by: Deborah Stephens, Bureau Chief Privacy Officer

- ☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- ☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

 Digitally signed by BRIAN ANDERSON
Date: 2026.04.20 18:28:44 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO DesignVision (DV)

Unique Project Identifier: PPL-PEC-02-00

Introduction: System Description

Provide a brief description of the information system.

DesignVision (DV) enables examiners working on patent applications to search images in a global Intellectual Property search dataset by using images as a query. Optionally, text can also be used as a query. DV uses non-generative Artificial Intelligence (AI) technologies.

DV compares uploaded images, including images from published and unpublished design applications, with Clarivate's global Intellectual Property search dataset and yields image results based on similarity. Clarivate's global Intellectual Property search dataset includes published (publicly-available) design patents, registrations, trademarks, and industrial designs from global Intellectual Property offices. United States Patent and Trademark Office (USPTO) employees and USPTO contractors can search, retrieve, and save content provided by the AI-powered image search tool in accordance with USPTO procedures. USPTO employees and USPTO contractors' access and interact with the system through the vendor's search interface.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system

Software as a Service (SaaS) image search application (non-major application)

(b) System location

Amazon Web Services (AWS) GovCloud (US) (East Region- Virginia)

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

The system interconnects with:

ICAM Identity as a Service (ICAM-IDaaS) - provides authentication and authorization for USPTO employees and USPTO contractors accessing DesignVision.

Enterprise Software Services (ESS) - Provides account management (creation, modification, disabling, auditing) for USPTO employees and USPTO contractors.

Identity Management Authenticator (ID-AUTH)- Provides identity management authenticators (e.g., Personal Identity Verification (PIV) cards) for USPTO employees and USPTO contractors.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

USPTO employees and USPTO contractors' access and interact with the system through the vendor's search interface. USPTO employees and USPTO contractors upload images, including images from published and unpublished design applications, and the system compares uploaded images with Clarivate's global Intellectual Property search dataset and yields image results based on similarity. USPTO employees and USPTO contractors can search, retrieve, and save content provided by the AI-powered image search tool in accordance with USPTO procedures.

(e) How information in the system is retrieved by the user

USPTO employees and USPTO contractors' access, search, and retrieve information via the vendor's search interface (i.e., portal).

(f) How information is transmitted to and from the system

Information is transmitted to and from the system via Hypertext Transfer Protocol Secure (HTTPS).

(g) Any information sharing

USPTO employees and USPTO contractors have the ability to export search reports which may be attached to patent applications or shared within the bureau on a case-by-case basis. Images uploaded by USPTO employees and USPTO contractors are redacted from exported search reports.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

USC Title 35 Part I and Part II

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- ☐ This is a new information system.
- ☐ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☐
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify):					

- ☐ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.
- ☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	☐	f. Driver's License	☐	j. Financial Account	☐
b. Taxpayer ID	☐	g. Passport	☐	k. Financial Transaction	☐
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
d. Employee ID	☐	i. Credit Card	☐	m. Medical Record	☐
e. File/Case ID	☐				
n. Other identifying numbers (specify): Patent Application Number and Patent Registration Number					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	☒	h. Date of Birth	☐	o. Financial Information	☐
b. Maiden Name	☐	i. Place of Birth	☐	p. Medical Information	☐
c. Alias	☐	j. Home Address	☐	q. Military Service	☐
d. Sex	☐	k. Telephone Number	☐	r. Criminal Record	☐
e. Age	☐	l. Email Address	☐	s. Marital Status	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☐	n. Religion	☐		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☐	e. Work Email Address	☐	i. Business Associates	☐
b. Job Title	☐	f. Salary	☐	j. Proprietary or Business Information	☒
c. Work Address	☐	g. Work History	☐	k. Procurement/contracting records	☐
d. Work Telephone Number	☐	h. Employment Performance Ratings or other Performance Information	☐		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	f. Scars, Marks, Tattoos	☐	k. Signatures	☐
b. Palm Prints	☐	g. Hair Color	☐	l. Vascular Scans	☐
c. Voice/Audio Recording	☐	h. Eye Color	☐	m. DNA Sample or Profile	☐
d. Video Recording	☐	i. Height	☐	n. Retina/Iris Scans	☐
e. Photographs	☐	j. Weight	☐	o. Dental Profile	☐
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☐
b. IP Address	☐	f. Queries Run	☒	f. Contents of Files	☐
g. Other system administration/audit data (specify):					

Other Information (specify)					

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	☐	Hard Copy: Mail/Fax	☐	Online	☐
Telephone	☐	Email	☐		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☐
State, Local, Tribal	☐	Foreign	☐		
Other (specify):					

Non-government Sources					
Public Organizations	☐	Private Sector	☐	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify): Clarivate global Intellectual Property search dataset					

2.3 Describe how the accuracy of the information in the system is ensured.

The accuracy of the information in the system is ensured by Clarivate's global Intellectual Property search dataset which currently covers 69 jurisdictions that are obtained and updated from a variety of sources. Each of these jurisdictions is checked for updates on at least a weekly basis, while some large registers like the United States (US) and Japan are checked daily. Because data updates consistency and frequency vary among Intellectual Property offices, data is not always added or changed as frequently for each register, but it is always checked so that new or updated data is reflected in the system on a regular basis. The system is secured using appropriate administrative physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screening
--

2.4 Is the information covered by the Paperwork Reduction Act?

☒	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0651-0032 Initial Patent Applications
☐	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

☒	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
-------------------------------------	--

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify): Click or tap here to enter text.			

☒	There are not any IT system supported activities which raise privacy risks/concerns.
-------------------------------------	--

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program	☐	For administering human resources programs	☐
For administrative matters	☒	To promote information sharing initiatives	☐
For litigation	☐	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☒	For employee or customer satisfaction	☒
For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
Other (specify):			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

Images from patent applications, including published and unpublished design applications, are uploaded into the system by examiners and used as queries for search. Uploaded images are automatically removed from the system upon completion of the examiner's user session.

Search results are public intellectual property records and include names (of people and/or businesses) for owners, agents, and designers. Data sources for these public intellectual property records are configured and maintained by the SaaS vendor (Clarivate). Data sources include design patents, registrations, trademarks, and industrial designs from global Intellectual Property offices and are updated by the SaaS vendor (Clarivate) at least once per week.

Examiners have the ability to export search reports. Examiners may be required to attach search reports to patent applications. Search reports may be shared within the bureau on a case-by-case basis. Images uploaded by USPTO employees and USPTO contractors are redacted from exported search reports, this precludes unauthorized disclosure of unpublished patent application information on the search reports.

The system uses the User ID of USPTO employees and USPTO contractors accessing the system for purposes of authentication and authorization.

DV collects audit logs, as indicated in section 2.1 of this PIA about individuals who have access to DV, this includes USPTO employees and USPTO contractors.

- 5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application, and all personnel who access the data must first authenticate to the system at which time an audit trail is generated. The SaaS vendor (Clarivate) adheres to the FedRAMP Continuous Monitoring Strategy & Guide and security logs are configured to send logs to Elastic SEIM which are continuously monitored for indicators of attack, unauthorized connections, and unauthorized use. Also, system users undergo annual mandatory training regarding appropriate handling of information.

NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	☒	☐	☒
DOC bureaus	☐	☐	☐
Federal agencies	☐	☐	☐
State, local, tribal gov't agencies	☐	☐	☐
Public	☐	☐	☐
Private sector	☐	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify): Patent Applicant	☒	☐	☐

☐ The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

☒	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

☒	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: ICAM-IDaaS ESS ID-AUTH NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.
☐	No, this IT system does not connect with or receive information from a nother IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	☐	Government Employees	☒
Contractors	☒		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

☒	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☒	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: The PIA serves as notice.
☐	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

☐	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: The individual does not have the opportunity to decline to provide PII/BII as it is required as part of the patent application and publication process.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

☐	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The individual does not have the opportunity to consent to particular uses of their PII/BII as it is only used as part of the patent application and publication process.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

☐	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: The individuals do not have an opportunity to review/update PII/BII pertaining to them as this is not the sources system and not available to the public. For publish patents, the individuals should contact the appropriate patent office to update their published patent and for USPTO employees they can contact HR to review/ update their PII.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that*

apply.)

☒	All users signed a confidentiality agreement or non-disclosure agreement.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: audit logs
☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 10/23/2024 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish DOC ownership rights over data including PII/BII.
☐	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. All access has role-based restrictions and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g. name or Social Security number)?

☒ Yes, the PII/BII is searchable by a personal identifier.

☐ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> COMMERCE-PAT-TM- 7 – Patent Application Files COMMERCE-DEPT-25 – Access control and Identity Management System
☐	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
☐	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

[General Records Schedules \(GRS\) / National Archives](#)

☒	There is an approved record control schedule. Provide the name of the record control schedule: Evidentiary Patent Applications N1-241-10-1:4.1 Patent Examination Working Files N1-241-10-1:4.2 Patent Examination Feeder Records N1-241-10-1:4.4 Patent Post-Examination Feeder Records N1-241-10-1:4.5 Patent Case Files, Granted N1-241-10-1:2 Abandoned Patent Applications, Not Referenced in Granted Case File N1-241-10-1:3
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.
☐	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	☐	Overwriting	☐

Degaussing	☐	Deleting	☒
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

☒	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☐	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

☒	Identifiability	Provide explanation: Names of owners, agents, and designers from public intellectual property records can be used to identify those specific individuals. User IDs for USPTO employees and USPTO contractors accessing the system can be used to identify those specific individuals.
☒	Quantity of PII	Provide explanation: Names of owners, agents, and designers from public intellectual property records number in the millions. User IDs for USPTO employees and USPTO contractors accessing the system will initially number in the hundreds, and are expected to eventually number in the thousands.
☒	Data Field Sensitivity	Provide explanation: Names of owners, agents, and designers from public intellectual property records are published by various global Intellectual Property offices and are not particularly sensitive. User IDs for USPTO employees and USPTO contractors accessing the system can be used to identify those specific individuals, but does not contain particularly sensitive fields such as SSN, medical history, or financial account information.
☒	Context of Use	Provide explanation: Names of owners, agents, and designers from public intellectual property records are used to process patent applications. User IDs for USPTO employees and USPTO contractors accessing the system are used for authentication and authorization.
☒	Obligation to Protect Confidentiality	Provide explanation: NIST Special Publication (SP) 800-122 and

		NIST SP 800-53 Revision 5 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M); Privacy Act of 1974.
☒	Access to and Location of PII	Provide explanation: PII within the system is accessed by USPTO employees and USPTO contractors. The SaaS vendor (Clarivate) hosts their cloud service offering in Amazon Web Services (AWS) GovCloud (US).
☐	Other:	Provide explanation:

Section 12: Analysis

- 12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The PII in this system poses a risk if exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. The SaaS vendor (Clarivate) adheres to the FedRAMP Continuous Monitoring Strategy & Guide and security logs are configured to send logs to Elastic Security Information and Event Management which are continuously monitored for indicators of attack, unauthorized connections, and unauthorized use.

- 12.2 Indicate whether the conduct of this PIA results in any required business process changes.

☐	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	No, the conduct of this PIA does not result in any required business process changes.

- 12.3 Indicate whether the conduct of this PIA results in any required technology changes.

☐	Yes, the conduct of this PIA results in required technology changes. Explanation:
--------------------------	--

☒	No, the conduct of this PIA does not result in any required technology changes.
--	---